VARIETIES OF NILPOTENT GROUPS OF CLASS FOUR

Patrick Fitzpatrick

Thesis submitted to the

Australian National University

for the

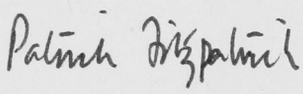
Degree of Doctor of Philosophy

Canberra

April 1980

To Johanna

The work in this thesis is my own except where otherwise stated.



Patrick Fitzpatrick

ACKNOWLEDGEMENTS

I am greatly indebted to my supervisor Laci Kovács for his constant and patient assistance and advice throughout the preparation of this thesis.

I gratefully acknowledge the financial support of the Australian National University from October 1976 to September 1979.

Finally, I thank Mrs Barbara Geary for her excellent typing.

ABSTRACT

All varieties of nilpotent groups of class at most 3 have been known for many years (Jonsson, Remeslennikov). In a preprint written jointly with L.G. Kovács, we have reduced to two cases the problem of determining all varieties of nilpotent groups of class at most 4 . The first is to deal with all such varieties whose free groups have no elements of order 2 : this is completed in that preprint. Part of the result is that those varieties form a distributive lattice with respect to inclusion order (though some joins in this lattice are different from joins formed in the lattice of all varieties).

The subject of this thesis is the second half of the problem: varieties whose free groups have no nontrivial elements of odd order. These do form a sublattice in the lattice of all varieties, but this sublattice is not distributive and so its description is considerably more complicated than the cases which were handled previously.

The main result assigns to each of our varieties a vector of 16 parameters, each parameter a nonnegative integer or ∞ , subject to simple but numerous conditions. Each parameter vector satisfying these conditions is in fact used (precisely once), and directly yields a (finite) defining set of laws for the variety it labels. One can read off the parameters whether one variety is contained in another.

Indeed, one can calculate the parameters of the join and the meet of two varieties from the parameters of the two components; algorithms for these calculations are presented (without proof) in an appendix. Given a variety $\underline{\underline{V}}$ by its parameters, it is easy to write down the parameters of the subvariety generated by the torsionfree groups of $\underline{\underline{V}}$, and to give an

upper estimate for the exponents of the torsion subgroups of the free groups of $\underline{\underline{V}}$. (These are necessary for making the reduction described in our preprint fully effective.)

Actually, all this is done in the dual context of fully invariant subgroups of the rank 4 free nilpotent group of class 4. The hardest part of the work is to deal with fully invariant subgroups contained in the last nontrivial term of the lower central series. This part also allows another interpretation, which may be of independent interest. Consider the free Lie algebra L of rank 4 over the ring of rational 2-adic integers, and let W be the homogeneous component of degree 4 in L. Let E be the subalgebra of the endomorphism algebra of W generated by the restrictions of the graded endomorphisms of L. We determine (the Morita-type of) E and the E-submodules of W.

CONTENTS

STATEMENT .. .. (i)

ACKNOWLEDGEMENTS .. .. (ii)

ABSTRACT .. .. (iii)

1. INTRODUCTION 1

2. ASSOCIATIVE RINGS 6

3. THE LIE MODULES 19

4. IDEMPOTENTS AND FURTHER REDUCTION 31

5. SUBMODULES OF U AND V 51

6. SUBMODULE STRUCTURE OF $U \oplus V$ 57

7. SUBMODULE STRUCTURE OF W 63

8. THE LAST TERM OF F 68

9. THE COMMUTATOR SUBGROUP F' 72

10. THE FINAL RESULT 75

APPENDIX 82

REFERENCES 87

1.

INTRODUCTION

This thesis is a report on the second half of a project aimed at determining all varieties of nilpotent groups of class at most 4 . The first half was carried out jointly by L.G. Kovács and the author, and is presented in an attached preprint [5]. There we show that the problem splits into two parts, the case of 2-torsionfree varieties (that is, varieties whose free groups have no elements of order 2) and the case of 2′-torsionfree varieties (whose free groups have no nontrivial elements of odd order). The first case is dealt with completely in that preprint; the second is the subject of this thesis.

Only two details from that paper will be relevant here. The first is that the 2′-torsionfree varieties form a sublattice within the lattice of all varieties of nilpotent groups of class at most 4 . The second is the list of torsionfree varieties (that is, varieties whose free groups are torsionfree) within this lattice. In the notation of Hanna Neumann's book [14], these are $\underline{\underline{E}}$, $\underline{\underline{A}}$, $\underline{\underline{N}}_2$, $\underline{\underline{N}}_3$, $\underline{\underline{A}}^2 \cap \underline{\underline{N}}_4$, $\underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4$, and $\underline{\underline{N}}_4$ itself.

As usual, all the work is carried out in the dual context: we consider 2′-isolated fully invariant subgroups in the rank 4 free group F of $\underline{\underline{N}}_4$. (A normal subgroup is called 2′-isolated if its factor group has no nontrivial element of odd order, and isolated if its factor group is torsionfree.) A nontrivial 2′-isolated fully invariant subgroup must have 2-power index in one of the six nontrivial isolated fully invariant subgroups of F ; this provides a natural subdivision of our task into six parts.

Let $\{x, y, z, t\}$ be a free generating set of F. We make much use of certain distinguished endomorphisms of F, namely: the 24 which permute these free generators; the endomorphism which maps x to xy and leaves each of y, z, t fixed; and, for each integer κ, the endomorphism which maps x to x^{κ} and leaves y, z, t fixed. The restrictions of these endomorphisms generate the semigroup of all endomorphisms of the commutator factor group F/F'. Again and again, we choose 2'-isolated fully invariant subgroups A, B in F such that $A \geq B$, the quotient A/B is abelian, and any two endomorphisms of F which agree on F/F' also agree on A/B. (For example, take A and B as successive terms of the lower central series of F.) In such a case, a subgroup between A and B is fully invariant in F if and only if it admits the distinguished endomorphisms listed above. In fact, as a group with the endomorphisms of F as operators, A/B may as well be viewed as a module for the semigroup of all endomorphisms of F/F'. With reference to the basis $\{xF', yF', zF', tF'\}$ of F/F', that semigroup is just the multiplicative semigroup $\mathrm{Mat}^{\times}(4, \mathbb{Z})$ of all 4×4 matrices with integer entries. As our interest lies in the 2'-isolated submodules of A/B, it is convenient to tensor A/B (over $\mathbb{Z}$) with the ring $\mathbb{Z}_2$ of rational 2-adic integers (vulgar fractions with odd denominators), and look for all submodules in this tensor product. Thus we end up investigating submodules of modules over the semigroup algebra $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})$.

The hardest cases are the modules obtained from $B = 1$ and A one of the verbal subgroup of F corresponding to $\underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4$, $\underline{\underline{A}}^2 \cap \underline{\underline{N}}_4$, and $\underline{\underline{N}}_3$. We denote these $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})$-modules by U, V, W, respectively. They are $\mathbb{Z}_2$-free of ranks 45, 15, 60; the direct sum $U \oplus V$ is contained in W as a submodule of 2-power index. The submodule lattices

of U and V are distributive, but that of W is not (because U and V do have isomorphic sections). The descriptions we obtain for their submodules are complete but far too complicated to present in this introduction. As an unexpected bonus, we could obtain complete descriptions of the quotients of $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})$ modulo the annihilators of U, V, or W. These are much easier to state, as follows.

With respect to a suitable $\mathbb{Z}_2$-basis of V, the quotient modulo the annihilator of V consists of all the 15×15 matrices over $\mathbb{Z}_2$ whose last row entries and last column entries, except perhaps the bottom right corner entry, are all divisible by 2. From this, it is easy to identify the submodules of V. One way of putting the essential part of this is to say that $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})/\mathrm{Ann}\ V$ is Morita equivalent to the ring of all 2×2 matrices over $\mathbb{Z}_2$ with even entries off the diagonal, and in this equivalence V corresponds to the free $\mathbb{Z}_2$-module on which this 2×2 matrix ring naturally acts. To make things even more compact: put $b = (b(i, j)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; then our 2×2 matrix ring consists of all (r_{ij}) with $r_{ij} \in 2^{b(i,j)}\mathbb{Z}_2$. The result for U is entirely similar, with

$$a = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 \end{pmatrix}$$

in place of b. Moreover, $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})/\mathrm{Ann}\ U \oplus V$ is Morita equivalent to to the ring of all 7×7 matrices (r_{ij}) such that

$$r_{ij} \in 2^{a(i,j)}\mathbb{Z}_2 \ , \quad r_{5+i,5+j} \in 2^{b(i,j)}\mathbb{Z}_2 \ ,$$

$$r_{ij} = 0 \quad \text{if} \quad i \leq 5 < j \quad \text{or} \quad i > 5 \geq j \ ,$$

$$r_{44} \equiv r_{66} \ , \quad r_{45} \equiv r_{67} \ , \quad r_{54} \equiv r_{76} \bmod 4 \ ,$$

and

$$r_{55} \equiv r_{77} \bmod 2 \ .$$

The submodules of $U \oplus V$ are read off this. Finally, recall that $U \oplus V \leq W$; in fact, $W \cong 4W \leq U \oplus V$, so once $4W$ is identified in terms of the description of the submodules of $U \oplus V$, one also has the result for W .

Working out all this takes up most of the space, even though tedious details of calculations are suppressed. When we move on to other choices of A/B , we verify that endomorphisms of F which agree on F/F' must agree on A/B , and then merely state the outcome of the consequent analysis of the submodule structure of A/B .

The end result is that each $2'$-torsionfree subvariety of $\underline{\underline{N}}_4$ is labelled by a vector of 16 parameters, each parameter a nonnegative integer or ∞ , subject to simple but numerous conditions. Each parameter-vector satisfying these conditions is in fact used (precisely once), and directly yields a defining set of laws for the variety it labels. One can recognise from the parameters whether one variety is contained in another. Joins and meets may also be calculated in terms of these parameters, but this calls for quite complicated algorithms which are therefore relegated to an appendix and their proofs are omitted.

Some of the results admit another interpretation. Namely, via the Magnus-Witt argument elaborated in Section 3 of Kovács [9], W may be

identified with the homogeneous component of degree 4 in a free Lie algebra L of rank 4 over $\mathbb{Z}_2$, and $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})/\mathrm{Ann}\, W$ with the $\mathbb{Z}_2$-subalgebra of $\mathrm{End}_{\mathbb{Z}_2} W$ generated by the restrictions of the graded endomorphisms of L. (In fact, for ease of notation we work most of the time in this setting.) So the $\mathbb{Z}_2$-algebra arising in this Lie context is Morita equivalent to the ring of 7×7 matrices described above, and the submodules of W are just the $\mathbb{Z}_2$-submodules of L which are homogeneous of degree 4 and admit all graded endomorphisms of L.

2.

ASSOCIATIVE RINGS

We start our preparations by collecting facts concerning associative rings, first in a general setting and then gradually focussing on $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z})$. Each associative ring considered will have a (multiplicative) identity element, normally denoted 1 , which acts identically on all the modules we look at. For such a ring R , we denote by $\mathrm{Mat}(n, R)$ the ring of all $n \times n$ matrices over R . The symbol $e_n(i, j)$ stands for the $n \times n$ "elementary" matrix whose entries are all 0 except the (i, j) entry which is 1 : the context should make it clear which ring 0 and 1 are to be taken from. The $n \times n$ identity matrix may be denoted by I_n if necessary, but more usually just by 1 . The "diagonal" matrix $\mathrm{diag}(r_1, \ldots, r_n)$ is the $n \times n$ matrix with (i, i) entry r_i (for $1 \leq i \leq n$) and all other entries 0 .

2.1 **PROPOSITION.** *Let R be an associative ring, ε an idempotent element of R such that $R\varepsilon R = R$, and M any right R-module. Then the lattice $S(M)$ of submodules of M is isomorphic to the lattice $S(M\varepsilon)$ of submodules of the $\varepsilon R\varepsilon$-module $M\varepsilon$.*

Proof. The assumption $R\varepsilon R = R$ means that the identity 1 of R may be written as a finite sum $\sum a_i \varepsilon b_i$ with $a_i, b_i \in R$. Define

$$\varphi : S(M) \to S(M\varepsilon) , \quad X \mapsto X\varepsilon ,$$

$$\psi : S(M\varepsilon) \to S(M) , \quad Y \mapsto YR .$$

If $X \in S(M)$ and $x \in X$, we have $x = x \sum a_i \varepsilon b_i = \sum x a_i \varepsilon b_i$; as $x a_i \in X$, this shows $x \in X\varepsilon R$. Thus $X\varepsilon R \geq X$. The converse inclusion is obvious, so $X\varepsilon R = X$, and $\varphi\psi$ is the identity map on $S(M)$. If $Y \in S(M\varepsilon)$, then $Y = Y\varepsilon$ (because $\varepsilon^2 = \varepsilon$) and so $Y = Y\varepsilon R\varepsilon = YR\varepsilon$: thus $\psi\varphi$ is the identity on $S(M\varepsilon)$. It is clear that φ and ψ preserve order, and well known that any poset-isomorphism of lattices is a lattice isomorphism. //

2.2 **Remark.** If $Y \in S(M\varepsilon)$ and Y is an $\varepsilon R\varepsilon$-generating set for Y, then Y is also an R-generating set for YR.

Such an idempotent will frequently arise from a ring homomorphism

$$\bigoplus_{k=1}^{s} \mathrm{Mat}\big(n(k), \mathbb{Z}\big) \to R .$$

Giving a homomorphism like this amounts to specifying elements ε_{ij}^k in R, with k ranging from 1 to s while for any fixed value of k the subscripts i, j range from 1 to $n(k)$, satisfying the relations

2.3 $$\varepsilon_{ij}^k \varepsilon_{lm}^n = \delta_{kn}\delta_{jl}\varepsilon_{im}^k$$

(where δ_{kn} and δ_{jl} are Kronecker deltas). Without loss of generality we may take

2.4 $$\sum\sum \varepsilon_{ii}^k = 1 :$$

for if this is not the case we put $\varepsilon_{11}^{s+1} = 1 - \sum\sum \varepsilon_{ii}^k$ and extend the range of the superscript k. Then define ε as

2.5 $$\varepsilon = \sum \varepsilon_{11}^{k} .$$

Clearly, ε is an idempotent, and

$$1 = \sum\sum \varepsilon_{ii}^{k} = \sum\sum \varepsilon_{i1}^{k}\varepsilon\varepsilon_{1i}^{k}$$

shows that $R\varepsilon R = R$, so 2.1 may be applied with this choice of ε.

The next result shows how, if ε is so chosen, a generating set of R leads to a generating set for $\varepsilon R\varepsilon$.

2.6 **LEMMA.** *Suppose the subset G of R generates R, and* 2.3, 2.4, 2.5 *hold. Then the set*

$$\bigcup_{i,j,k,m} \varepsilon_{1i}^{k} G \varepsilon_{j1}^{m}$$

generates $\varepsilon R\varepsilon$. Similarly, if R is an algebra over a commutative ring K with 1 and G generates R as K-algebra, the given set generates $\varepsilon R\varepsilon$ as K-algebra.

Proof. We need to show that if p is any product of elements of G then $\varepsilon p\varepsilon$ is a sum of products of elements of the set proposed to generate $\varepsilon R\varepsilon$. When p is just rs with $r, s \in G$, we have that

$$\varepsilon p\varepsilon = \varepsilon rs\varepsilon = \left(\sum \varepsilon_{11}^{l}\right) r \left(\sum\sum\sum \varepsilon_{i1}^{k}\varepsilon_{1i}^{m}\right) s \left(\sum \varepsilon_{11}^{n}\right) ,$$

since the middle factor on the right hand side is 1. This is a sum of products of the $\varepsilon_{11}^{l} r \varepsilon_{i1}^{k}$ and $\varepsilon_{1i}^{m} s \varepsilon_{11}^{n}$, each of which lies in the proposed generating set. When $p \in G$ or p is a product of more than two factors from G, the argument follows the same pattern. //

The ring we shall need will be a semigroup algebra. For a commutative (and associative) ring K with 1 and a semigroup G with zero, the (contracted) semigroup algebra KG is the K-module freely generated by the

nonzero elements of G, with multiplication defined by K-linear extension of the multiplication in G, after the identification of the zero of G with the zero of the module KG. Explicitly, the elements of KG are the formal expressions $\sum \kappa_g g$ with summation over all nonzero g in G, the κ_g elements of K, all but finitely many of them zero. They are manipulated according to the rules

$$\kappa \sum \alpha_g g + \sum \beta_g g = \sum (\kappa\alpha_g + \beta_g) g$$

and

$$\left(\sum \alpha_g g\right)\left(\sum \beta_g g\right) = \sum (\gamma_g g)$$

where $\gamma_g = \sum \alpha_{g'}\beta_{g''}$, summation being over all ordered pairs (g', g'') with $g'g'' = g$. We identify the nonzero elements of G and the formal expressions with one coefficient 1 and all other coefficients 0. Thus if G has an identity element, that is also the identity element of KG.

From now on G will denote $\mathrm{Mat}^{\times}(4, \mathbb{Z})$, the multiplicative semigroup of all 4×4 integer matrices. Special care must be taken to remember that *every time* we write down a linear combination of elements of G, we mean the corresponding formal expression in the semigroup algebra, *not* in the ring $\mathrm{Mat}(4, \mathbb{Z})$. For instance, in this context

$$-\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \neq \begin{pmatrix} -1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix} !$$

Before we start contemplating the semigroup algebra, we establish a

fact which will be fundamental to our work, used most of the time, usually without reference.

2.7 PROPOSITION. *The semigroup* G *is generated by the set* G *which consists of the* 4×4 *permutation matrices, the diagonal matrices* μ_κ *defined by* $\mu_\kappa = \mathrm{diag}(\kappa, 1, 1, 1)$ *(one for each* κ *in* $\mathbb{Z}$*), and the matrix* τ *obtained from the* 4×4 *identity matrix by changing its* $(1, 2)$ *entry to* 1 .

Proof. This is based on the familiar fact that every integer matrix can be transformed to diagonal (or even to "Smith normal") form by invertible elementary row and column operations, that is, (note $\tau^{-1} = \mu_{-1}\tau\mu_{-1}$) by pre- and post-multiplication by products formed from τ, μ_{-1} , and permutation matrices. All diagonal matrices are obviously in the semigroup generated by the μ_κ and the permutation matrices; so our claim follows. //

It will lead to no confusion if we write 1 for the identity of G . We shall also write

$$\sigma_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

S_1 for the group consisting of 1 alone,

S_2 for the group generated by σ_2 ,

S_3 for the symmetric group generated by σ_2 and σ_3 , and

S_4 for the symmetric group generated by σ_2 and σ_4 .

We put $\partial_1 = \mu_0$ and $\partial_i = \sigma_i \partial_\emptyset \sigma_i^{-1}$ for $i = 2, 3, 4$; thus for instance $\partial_3 = \mathrm{diag}(1, 1, 0, 1)$.

Our next task is to identify elements in the semigroup algebra KG (where at this stage K is any commutative and associative ring with 1) which satisfy the relations 2.3. Of course, the $e_4(i, j)$ of G would always do, but as these annihilate the modules we shall be interested in, they are no help. So we must look for others; to this end, we exploit first the pairwise commuting idempotents $\partial_1, \ldots, \partial_4$. Formal expansion in KG gives

$$1 = \prod_{i=1}^{4} [(1-\partial_i)+\partial_i] = \sum_J \prod_{j\in J} (1-\partial_j) \prod_{i\notin J} \partial_i$$

with summation over all subsets J of $\{1, 2, 3, 4\}$. Put $\varepsilon_J = \prod_{j\in J} (1-\partial_j) \prod_{i\notin J} \partial_i$; the fact that the ∂_i are pairwise commuting idempotents immediately yields that the ε_J are pairwise orthogonal idempotents. As $\varepsilon_\emptyset = 0$, we restrict attention to nonempty J . It will be convenient to name the subsets $\{1, \ldots, i\}$ as Z_i , and to write ε_i for ε_{Z_i} .

For subsets I, J of equal cardinality, let $\sigma(I, J)$ denote that permutation of Z_4 which maps I to J preserving order, and $Z_4 \backslash I$ to $Z_4 \backslash J$ also preserving order; we shall write $\sigma(I, J)$ also for the corresponding permutation matrix. Note that $\sigma(I, J) = \sigma(J, I)^{-1}$. Next, define $\varepsilon(I, J)$ by $\varepsilon(I, J) = \varepsilon_I \sigma(I, J)$. We shall show that these

elements satisfy 2.3, but first we prove the following.

2.8 LEMMA. *Let* $\sigma \in S_4$. *Then* $\varepsilon_J \sigma = \sigma \varepsilon_{J\sigma}$.

Proof. It is clear that $\partial_i \sigma = \sigma \partial_{i\sigma}$ (note the dual use of the symbol σ); thus

$$\left[\prod_{j\in J}(1-\partial_j)\prod_{i\notin J}\partial_i\right]\sigma = \sigma\left[\prod_{j\in J}(1-\partial_{j\sigma})\prod_{i\notin J}\partial_{i\sigma}\right]$$

$$= \sigma\left[\prod_{j\in J\sigma}(1-\partial_j)\prod_{i\notin J\sigma}\partial_i\right],$$

and this is what we want. //

We shall make frequent use of this lemma and its obvious corollaries $\sigma\varepsilon_J = \varepsilon_{J\sigma^{-1}}\sigma$ and $\varepsilon(I, J) = \sigma(I, J)\varepsilon_J$, without specific reference.

2.9 PROPOSITION. *For all subsets* I, J, L, N *of* Z_4 ,

$$\varepsilon(I, J)\varepsilon(L, N) = \delta_{JL}\varepsilon(I, N)$$

(δ_{JL} *a Kronecker* δ).

Proof.

$$\varepsilon(I, J)\varepsilon(L, N) = \varepsilon_I\sigma(I, J)\varepsilon_L\sigma(L, N)$$

$$= \sigma(I, J)\varepsilon_J\varepsilon_L\sigma(L, N)$$

and this is zero unless $J = L$. If this is the case then the cardinalities $|I|, |J|, |L|, |N|$ are all equal and

$$\varepsilon(I, J)\varepsilon(J, N) = \varepsilon_I\sigma(I, J)\varepsilon_J\sigma(J, N) = \sigma(I, J)\varepsilon_J\varepsilon_J\sigma(J, N)$$

$$= \sigma(I, J)\varepsilon_J\sigma(J, N) = \varepsilon_I\sigma(I, J)\sigma(J, N) = \varepsilon_I\sigma(I, N) = \varepsilon(I, N)$$

since $\sigma(I, J)\sigma(J, N) = \sigma(I, N)$. //

For an application of 2.3 and so on, we may view the $\varepsilon(I, J)$ as having subscripts I and J and the common cardinality of I and J as superscript. Since $J = L$ implies $|J| = |L|$ we may omit the superscript and the other Kronecker delta $\delta_{|J||L|}$ required in 2.3.

Observe that $\varepsilon(I, I) = \varepsilon_I\sigma(I, I) = \varepsilon_I$ since $\sigma(I, I)$ is the identity permutation, so

$$\sum_I \varepsilon(I, I) = \sum_I \varepsilon_I = 1 ,$$

corresponding to 2.4.

The obvious choices for the subsets corresponding to the subscript 1 in 2.5 are the initial subsets Z_i , $1 \le i \le 4$. Then for

$$\varepsilon = \sum_{i=1}^{4} \varepsilon_i$$

we have $(KG)\varepsilon(KG) = KG$ and thus we may apply 2.1.

The only remaining task is to describe explicitly the generating set of $\varepsilon KG\varepsilon$ obtained from G by 2.6.

2.10 **PROPOSITION.** *The union of the sets* $\varepsilon_i S_i \varepsilon_i$ $(1 \le i \le 4)$,

$$\{\varepsilon_i \mu_\kappa \varepsilon_i,\ \varepsilon_i \tau \varepsilon_i \mid 1 \le i \le 4,\ \kappa \in \mathbb{Z}\} ,$$

and

$$\{\varepsilon_i\tau\sigma(Z_i\backslash\{1\},\ Z_{i-1})\varepsilon_{i-1},\ \varepsilon_{j-1}\sigma(Z_{j-1},\ Z_j\backslash\{2\})\tau\varepsilon_j \mid 2 \le i, j \le 4\}$$

generates $\varepsilon KG\varepsilon$.

Proof. We know from 2.6 that $\varepsilon KG\varepsilon$ is generated by

$$\bigcup_{I,J} \varepsilon(Z_{|I|},\ I)G\varepsilon(J,\ Z_{|J|}) ,$$

so it suffices to show that all nonzero elements of this set occur among the proposed generators. Just for this proof, write $|I|$ as i and $|J|$ as j . We consider $\varepsilon(Z_i,\ I)S_4\varepsilon(J,\ Z_j)$, $\varepsilon(Z_i,\ I)\mu_K\varepsilon(J,\ Z_j)$ and $\varepsilon(Z_i,\ I)\tau\varepsilon(J,\ Z_j)$ in turn.

Firstly:

$$\varepsilon(Z_i,\ I)S_4\varepsilon(J,\ Z_j) = \varepsilon_i\sigma(Z_i,\ I)S_4\sigma(J,\ Z_j)\varepsilon_j = \varepsilon_i S_4\varepsilon_j .$$

Let $\sigma \in S_4$ and $\varepsilon_i\sigma\varepsilon_j \neq 0$. As $\varepsilon_i\sigma\varepsilon_j = \sigma\varepsilon_L\varepsilon_j$ with $L = Z_i\sigma$, we must have $Z_i\sigma = Z_j$, so $j = i$ and σ leaves Z_i (setwise) fixed. Therefore it is possible to write $\sigma = \sigma'\sigma''$ where σ' leaves each element of Z_i fixed and $\sigma'' \in S_i$. Now ε_i is, by its definition, a multiple of $\prod_{j>i} \partial_j$, and direct multiplication shows $\left(\prod_{j>i} \partial_j\right)\sigma' = \prod_{j>i} \partial_j$: thus $\varepsilon_i\sigma' = \varepsilon_i$ and so $\varepsilon_i\sigma\varepsilon_i = \varepsilon_i\sigma''\varepsilon_i$. This proves that $\varepsilon_i S_4\varepsilon_j \subseteq \{0\} \cup \varepsilon_i S_i\varepsilon_i$.

Secondly: observe that μ_K commutes with each ∂_k and hence also with each ε_I , and with all permutations that fix 1 . Thus

$$\varepsilon(Z_i, I)\mu_K\varepsilon(J, Z_j) = \varepsilon_i\sigma(Z_i, I)\mu_K\varepsilon_J\sigma(J, Z_j) = \sigma(Z_i, I)\mu_K\varepsilon_I\varepsilon_J\sigma(J, Z_j)$$

and this is zero unless $I = J$. Now if $1 \notin I$ then $\partial_1\mu_K = \partial_1$ yields that $\varepsilon_I\mu_K = \varepsilon_I$, and so

$$\varepsilon(Z_i, I)\mu_K\varepsilon(I, Z_i) = \sigma(Z_i, I)\varepsilon_I\mu_K\varepsilon(I, Z_i) = \varepsilon(Z_i, I)\varepsilon(I, Z_i) = \varepsilon_i \in \varepsilon_i S_i \varepsilon_i .$$

On the other hand, if $1 \in I$ then $\sigma(I, Z_i)$ fixes 1 and so commutes with μ_K : hence

$$\varepsilon(Z_i, I)\mu_K\varepsilon(I, Z_i) = \varepsilon_i\sigma(Z_i, I)\mu_K\sigma(I, Z_i)\varepsilon_i = \varepsilon_i\mu_K\varepsilon_i .$$

Thirdly: observe that τ commutes with all permutations that fix 1 and 2 and also with ∂_3 and ∂_4 . Moreover, $\partial_1\tau = \partial_1$, $\tau\partial_2 = \partial_2$ and $\partial_2\tau\partial_1 = \partial_2\sigma_2\partial_1$ (recall σ_2 is the permutation which interchanges 1 and 2 and fixes 3 and 4).

Writing $\varepsilon(Z_i, I)\tau\varepsilon(J, Z_j)$ in the form $\sigma(Z_i, I)\varepsilon_I\tau\varepsilon_J\sigma(J, Z_j)$ we see that if $1 \notin I$ then ε_I has a factor ∂_1 so τ is redundant; if $2 \notin J$ then ε_J has a factor ∂_2 so τ is again redundant; if $2 \notin I$ and $1 \notin J$ then $\varepsilon_I\tau\varepsilon_J$ has a factor $\partial_2\tau\partial_1$ so this generator belongs to $\varepsilon(Z_i, I)S_4\varepsilon(J, Z_j)$; and, finally, if $I\backslash\{1, 2\} \neq J\backslash\{1, 2\}$ then $\varepsilon_I\tau\varepsilon_J$ has a factor $(1-\partial_3)\partial_3$ or $(1-\partial_4)\partial_4$ and so is zero.

Thus the following cases remain for consideration:

(i) $\{1, 2\} \subseteq I = J$,

(ii) $\{1, 2\} \subseteq I$ and $J = I\backslash\{1\}$,

(iii) $\{1, 2\} \subseteq J$ and $I = J\backslash\{2\}$.

In cases (i) and (ii), $\sigma(Z_i, I)$ fixes 1 and 2 and hence commutes with τ, so we have

$$\varepsilon(Z_i, I)\tau\varepsilon(J, Z_j) = \varepsilon_i\tau\sigma(Z_i, I)\sigma(I, Z_i)\varepsilon_i = \varepsilon_i\tau\varepsilon_i$$

and

$$\varepsilon(Z_i, I)\tau\varepsilon(J, Z_j) = \varepsilon_i\tau\sigma(Z_i, I)\sigma(I\backslash\{1\}, Z_{i-1})\varepsilon_{i-1} = \varepsilon_i\tau\sigma(Z_i\backslash\{1\}, Z_{i-1})\varepsilon_{i-1}$$

respectively.

In case (iii), $\sigma(J, Z_j)$ commutes with τ so we have

$$\varepsilon(Z_i, I)\tau\varepsilon(J, Z_j) = \varepsilon_{j-1}\sigma(Z_{j-1}, J\backslash\{2\})\sigma(J, Z_j)\tau\varepsilon_j = \varepsilon_{j-1}\sigma(Z_{j-1}, Z_j\backslash\{2\})\tau\varepsilon_j .$$

(The products of the permutations in these last two calculations are tedious but straightforward consequences of the definitions.)

This completes the proof of the proposition. //

The symbols $\varepsilon_i\tau\sigma(Z_i\backslash\{1\}, Z_{i-1})\varepsilon_{i-1}$ and $\varepsilon_{j-1}\sigma(Z_{j-1}, Z_j\backslash\{2\})\tau\varepsilon_j$ are rather unwieldy so we shall abbreviate them to $(i \to i\text{-}1)$ and $(j\text{-}1 \to j)$, respectively. Also we note that $\varepsilon_1 S_1 \varepsilon_1 = \{\varepsilon_1\mu_1\varepsilon_1\}$, while $\varepsilon_i S_i \varepsilon_i$ is generated by $\varepsilon_i\sigma_2\varepsilon_i$ and $\varepsilon_i\sigma_i\varepsilon_i$ when $i = 2, 3$, or 4. Thus we have the following.

2.11 COROLLARY. *The union of*

$$\{\varepsilon_i\sigma_2\varepsilon_i,\ \varepsilon_i\sigma_i\varepsilon_i,\ (i\text{-}1 \to i),\ (i \to i\text{-}1) \mid 2 \le i \le 4\}$$

and

$$\{\varepsilon_i\mu_\kappa\varepsilon_i,\ \varepsilon_i\tau\varepsilon_i \mid 1 \le i \le 4,\ \kappa \in \mathbb{Z}\}$$

generates $\varepsilon KG\varepsilon$.

Further applications of 2.1 become possible when 3 is a unit in K , for then it is known that $KS_3 \cong KS_2 \oplus \mathrm{Mat}(2, K)$ and

$$\tfrac{1}{3}\left(1+\sigma_3+\sigma_3^2\right),\ \tfrac{1}{3}\left(1-\sigma_3-\sigma_2\sigma_3+\sigma_2\sigma_3^2\right),\ \tfrac{1}{3}\left(1-\sigma_3^2+\sigma_2\sigma_3-\sigma_2\sigma_3^2\right)$$

are pairwise orthogonal idempotents with sum 1 . (This is readily verified by direct calculation; see also Boerner's description in [2] of Young's "natural representation" for S_n .) We know from 2.8 that ε_3 and ε_4 commute with S_3 and so $r \longmapsto \varepsilon_i r \varepsilon_i$ $(i = 3, 4)$ define homomorphisms $KS_3 \to \varepsilon_i KG\varepsilon_i$. Thus $\varepsilon KG\varepsilon$ contains the direct sum $\varepsilon_3 KS_3 \varepsilon_3 \oplus \varepsilon_4 KS_3 \varepsilon_4$ of the homomorphic images $\varepsilon_i KS_3 \varepsilon_i$ of $KS_2 \oplus \mathrm{Mat}(2, K)$. In particular, we obtain 6 pairwise orthogonal idempotents with sum $\varepsilon_3 + \varepsilon_4$.

All this is available once we focus our attention on $\mathbb{Z}_2 G$ instead of the general KG (recall that $\mathbb{Z}_2$ stands for the ring of rational 2-adic integers), but a lot more will be needed. There is one more step which can be sketched before we begin investigating the action of $\mathbb{Z}_2 G$ on particular modules. This exploits the fact that, as we hinted before, ε_1 will annihilate all the modules we look at, so they may be viewed not only as $\mathbb{Z}_2 G$ or $\varepsilon \mathbb{Z}_2 G \varepsilon$ modules, respectively, but also as modules for the quotients of these rings modulo their (two-sided) ideals generated by ε_1 . Now the definitions of ε_1 and ε_2 give

$$\varepsilon_2 = \left(-\varepsilon_1 - \sigma_2 \varepsilon_1 \sigma_2\right) + \partial_3 \partial_4 ,$$

and we have already noted that $\partial_3 \partial_4$ commutes with μ_{-1}, σ_2 , and τ . The

semigroup H generated by σ_2 and $\sigma_2\mu_{-1}\tau$ is isomorphic to S_3. Thus

$$\mathbb{Z}_2S_2 \oplus \mathrm{Mat}(2, \mathbb{Z}_2) \cong \mathbb{Z}_2H \to \mathbb{Z}_2G/\mathbb{Z}_2G\varepsilon_1\mathbb{Z}_2G$$

defined by $r \mapsto \varepsilon_2 r\varepsilon_2 + \mathbb{Z}_2G\varepsilon_1\mathbb{Z}_2G$ is a ring homomorphism, and so is $\mathbb{Z}_2H \to \varepsilon\mathbb{Z}_2G\varepsilon/\varepsilon\mathbb{Z}_2G\varepsilon_1\mathbb{Z}_2G\varepsilon$, $r \mapsto \varepsilon_2 r\varepsilon_2 + \varepsilon\mathbb{Z}_2G\varepsilon_1\mathbb{Z}_2G\varepsilon$. This prepares the way for yet another application of 2.1. Unfortunately we find it necessary to take one even more *ad hoc* step before we get through. That, and what one would obtain from this paragraph and the last, will be telescoped into a single, complex move. The purpose of these two paragraphs has been to offer at least some partial motivation for what might otherwise appear a set of quite arbitrary choices, and to indicate the nature of some calculations which will be suppressed.

3.

THE LIE MODULES

This section sets the scene for the work which is the core of this thesis. Let L be the Lie algebra over $\mathbb{Z}_2$ freely generated by "the variables" x, y, z, t. This may be envisaged within the algebra A of all polynomials in these noncommuting variables, with coefficients from $\mathbb{Z}_2$. With respect to the usual Lie product $[u, v]$ defined as $uv - vu$, this is also a Lie algebra, and L is its Lie subalgebra generated by x, y, z, t. As we never deal with associative products here, we shall simply use juxtaposition for Lie products and omit left-normed brackets: thus we write xyz for $[[x, y], z]$. We shall be particularly interested in the set W of those elements of L which as polynomials are homogeneous of (total) degree 4; this is a $\mathbb{Z}_2$-module freely generated by the 60 basic Lie monomials of degree 4.

Our semigroup G $(= \mathrm{Mat}^{\times}(4, \mathbb{Z}))$ acts on A by (linear homogeneous) substitutions: (α_{ij}) mapping x to $\alpha_{11}x + \alpha_{12}y + \alpha_{13}z + \alpha_{14}t$, and so on. It is clear that W is a G-submodule of A, annihilated by the zero of G, so W is a module for the contracted semigroup algebra $\mathbb{Z}_2G$.

We note, though we shall never use, that W could be considered similarly as a $\mathbb{Z}_2\mathrm{Mat}^{\times}(4, \mathbb{Z}_2)$-module, without this change of view making any real difference. For, each element of $\mathrm{Mat}^{\times}(4, \mathbb{Z}_2)$ can be written as the product of an element g of G and a "scalar" matrix $\mathrm{diag}(\kappa, \kappa, \kappa, \kappa)$ with κ the reciprocal of an odd integer, and - as W consists of homogeneous polynomials of degree 4 - acts on W as the element $\kappa^4 g$ of

$\mathbb{Z}_2 G$. Thus $\mathbb{Z}_2 G$ and $\mathbb{Z}_2 \mathrm{Mat}^{\times}(4, \mathbb{Z}_2)$ are represented on W by the same set of $\mathbb{Z}_2$-endomorphisms. The only point of this observation is to justify a comment in the last paragraph of our Introduction, that $\mathbb{Z}_2 G/\mathrm{Ann}\, W$ is isomorphic to the subalgebra of $\mathrm{End}_{\mathbb{Z}_2} W$ generated by the restrictions of the graded endomorphisms of L . These graded endomorphisms are, of course, just the elements of $\mathrm{Mat}^{\times}(4, \mathbb{Z}_2)$ acting on L as linear homogeneous substitutions. We shall say no more about this aside; the interested reader will find the context explained in Wall [18] and more specifically in Section 3 of Kovács [9].

The reason we are interested in W is that the lattice $S(W)$ of its $\mathbb{Z}_2 G$-submodules is isomorphic to the lattice of those $2'$-isolated fully invariant subgroups of the rank 4 free group F of $\underline{\underline{\mathrm{N}}}_4$ which lie in the last nontrivial term of the lower central series of that group. Indeed, that bijection is not only a lattice isomorphism: it also matches isolated fully invariant subgroups of F with isolated submodules of W . In particular, it yields that corresponding to the two torsionfree varieties strictly between $\underline{\underline{\mathrm{N}}}_3$ and $\underline{\underline{\mathrm{N}}}_4$ (seen in the list quoted in the Introduction) there are precisely two isolated (proper nonzero) submodules in W . One of these, which we shall call U , contains $yxxy$, and the other, V , contains $(tx)(yz)$. All this is seen by the Magnus-Witt argument which is described in Section 3 of Kovács [9] in almost exactly the form we require; the argument is so well known, and what little adaptation it still needs is so obvious, that we do not repeat it here. We shall not need this connection again until we have completed the study of the submodules of W . In fact, we shall rederive rather than use the information just quoted about U and V ; the quote serves merely as motivation for turning our attention

to these submodules in W. It will be a by-product of our work that $yxxy$ in fact generates U, confirming the relevant part of a claim made without proof in the (unpublished) thesis [16] of Pentony.

The starting point for the study of W is the reduction we prepared in the previous section, based on the use of the idempotents ∂_i, ε_i, and ε, of $\mathbb{Z}_2G$. From the definition of the ∂_i it is immediate that each (Lie) monomial is either annihilated or left unchanged when we act on it by a ∂_i; so the same can be said for the $1 - \partial_i$, and hence also for the ε_i. In fact, a monomial must be annihilated by ε_i unless it is the (Lie) product of precisely the first i variables (in any order and any bracketing, repeated factors allowed): so to each monomial there is at most one exceptional ε_i. (Note that ε_1 must annihilate every monomial of degree 4, so $W\varepsilon_1 = 0$: this will be taken for granted without further reference.) It follows then that each monomial is either annihilated or fixed by ε. On examining each of the 60 basic monomials of degree 4 in turn, we find that 42 are annihilated by ε and 18 are left unchanged; these 18 will then form a $\mathbb{Z}_2$-basis for $W\varepsilon$. However, we shall find another basis more convenient to work with. The reason for this is that while the diagonal generators μ_κ of G act very simply on each monomial (multiplying it by κ^m where m is the degree of the monomial in x), the permutation matrices in G mix basic and nonbasic monomials. While this complication cannot be entirely avoided, one can do better than by using the basic monomials.

3.1 LEMMA. *The following sets are bases for the* $W\varepsilon_i$:

$W\varepsilon_2$: $\{yxxy, yxxx, xyyy\}$,

$W\varepsilon_3$: $\{yxxz,\ zxxy,\ (yx)(xz),\ zyyx,\ xyyz,\ (zy)(yx),\ xzzy,\ yzzx,\ (xz)(zy)\}$,

$W\varepsilon_4$: $\{txyz,\ tyzx,\ tzxy,\ (tx)(yz),\ (ty)(zx),\ (tz)(xy)\}$.

Proof. Recall that $W\varepsilon_1 = 0$ and, as $\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4$ and the ε_i are pairwise orthogonal, $W\varepsilon = W\varepsilon_2 \oplus W\varepsilon_3 \oplus W\varepsilon_4$. The three sets listed above lie in the relevant $W\varepsilon_i$, and their union has the right cardinality for a basis of $W\varepsilon$: this much is obvious. It is therefore sufficient to show that the union spans $W\varepsilon$. By the well-known argument usually referred to as Nakayama's Lemma, this will follow if we can show that the union spans $W\varepsilon$ modulo $2W\varepsilon$. There seems to be no easy method beyond this point; we just have to check one by one that each of the 18 basics fixed by ε is, modulo $2W\varepsilon$, in the span of the union. The routine details are omitted. //

The next natural and necessary step would be to calculate just how the generators of $\varepsilon\mathbb{Z}_2G\varepsilon$ (identified in 2.11) act on this basis of $W\varepsilon$. In practice it will be more profitable to display their action on another set of 18 elements which will turn out to be the union of convenient bases of $U\varepsilon$ and $V\varepsilon$. Define

$$a_1 = yxxy ,$$

$$a_2 = yxxx ,$$

$$a_3 = a_2\sigma_2 ,$$

$$a_4 = 3yxxz - zxxy - 3(yx)(xz) ,$$

$$a_5 = a_4\sigma_3 ,$$

$$a_6 = a_4\sigma_3^2 ,$$

$$a_7 = 4yxxz - 3(yx)(xz) ,$$

$$a_8 = a_7\sigma_3 ,$$

$$a_9 = a_7\sigma_3^2 ,$$

$$a_{10} = 2txyz - 2tyzx - 2tzxy - (tx)(yz) + 2(ty)(zx) ,$$

$$a_{11} = a_{10}\sigma_3 ,$$

$$a_{12} = a_{10}\sigma_3^2 ;$$

$$b_7 = (yx)(xz) ,$$

$$b_8 = b_7\sigma_3 ,$$

$$b_9 = b_7\sigma_3^2 ,$$

$$b_{10} = (tx)(yz) ,$$

$$b_{11} = b_{10}\sigma_3 ,$$

$$b_{12} = b_{10}\sigma_3^2 .$$

Some of the action is obvious. A quick inspection shows that, though not all these elements are monomials, each lies in some $W\varepsilon_i$ and is therefore annihilated by every generator which is a product with first factor another ε_j. Similarly, each of these elements is homogeneous in x, so if it lies in $W\varepsilon_i$ and has degree m in x then $\varepsilon_i\mu_\kappa\varepsilon_i$ will simply multiply it by the scalar κ^m. More can be said directly about the b_i: see 3.4 below. The rest of the action must be determined by straightforward, case-by-case calculation; the result is displayed in the tables at the end of this section. At this stage, we draw the following conclusions.

3.2 LEMMA. *Let U be the smallest isolated submodule of W containing $yxxy$. Then*

U is generated by $yxxy$;

the set $\{a_i \mid 1 \le i \le 3\}$ *is a basis for* $U\varepsilon_2$,

$\{a_i \mid 4 \le i \le 9\}$ *is a basis for* $U\varepsilon_3$, *and*

$\{a_i \mid 10 \le i \le 12\}$ *is a basis for* $U\varepsilon_4$.

Proof. The tables show that the union of these sets spans an $\varepsilon\mathbb{Z}_2G\varepsilon$-submodule in $W\varepsilon$. It is immediately visible from 3.1 and the definition of the a_i that these 12 elements are independent modulo $2W\varepsilon$; hence they form a basis for their span, and that span is isolated in $W\varepsilon$. The main step is to identify this span as $U\varepsilon$. By the definition of U , if $w \in U\varepsilon$ then $2^n w \in a_1\mathbb{Z}_2G$ for some nonnegative integer n . As $w\varepsilon = w$ and $a_1\varepsilon = a_1$, this means $2^n w \in a_1\varepsilon\mathbb{Z}_2G\varepsilon$. We have just seen that the span of the a_i is an isolated $\varepsilon\mathbb{Z}_2G\varepsilon$-submodule: so we may conclude that it contains $U\varepsilon$. For the converse, use the tables to verify that

$$a_2 = a_1(1-\varepsilon_2\tau\varepsilon_2)(\varepsilon_2\sigma_2\varepsilon_2) ,$$

$$a_4 = -a_1(2 \to 3)(\varepsilon_3\sigma_3\varepsilon_3)\left[1+(\varepsilon_3\tau\varepsilon_3-1)(\varepsilon_3\sigma_3\varepsilon_3)^2\right] ,$$

$$a_7 = a_4 - a_1(2 \to 3)(\varepsilon_3\sigma_3\varepsilon_3) ,$$

$$a_{10} = (a_4-a_7)(3 \to 4)(\varepsilon_4\sigma_4\varepsilon_4) .$$

Together with the definitions of the other a_i , these relations show that all the a_i lie in $a_1\mathbb{Z}_2G$ and hence in U ; as they are also in $W\varepsilon$, they are in $U\varepsilon$. The final point is that a_1 generates U as $\mathbb{Z}_2G$-module: we have just seen that it generates $U\varepsilon$ as $\varepsilon\mathbb{Z}_2G\varepsilon$-module, so this follows by 2.2. //

3.3 LEMMA. *Let* V *be the smallest isolated submodule of* W

containing $(tx)(yz)$. *Then the sets* $\{b_7, b_8, b_9\}$ *and* $\{b_{10}, b_{11}, b_{12}\}$ *are bases for* $V\varepsilon_3$ *and* $V\varepsilon_4$, *respectively; while* $V\varepsilon_2 = V(3 \to 2) = 0$.

Proof. This does not depend on the tables. It is easy to see that the $\mathbb{Z}_2G$-submodule of W generated by $(tx)(yz)$ contains all the monomials of degree 4 which are bracketed like $(tx)(yz)$, and that each $(tx)(yz)g$ with $g \in G$ is a $\mathbb{Z}_2$-linear combination of such monomials. Moreover, each such monomial is either basic or the negative of a basic, so the non-left-normed basics form a basis for this module, and this module is isolated: it is therefore V . Similarly, each such monomial fixed by ε is either a b_i or the negative of a b_i , while the b_i belong to the basis of $W\varepsilon$ given in 3.1: hence they form a basis for $V\varepsilon$. Finally, each of these monomials involves at least three variables and is therefore annihilated by ε_2 . As to $V(3 \to 2)$, recall that $(3 \to 2)$ is shorthand for a product with last factor ε_2 : since V is a submodule, this yields $V(3 \to 2) \leq V\varepsilon_2 = 0$. //

We conclude this section by the promised tables. It is easiest to explain how to read them by some examples: the first line of the first table means that $a_1(\varepsilon_2\sigma_2\varepsilon_2) = -a_1$; the middle line of the second table means $a_2(\varepsilon_2\tau\varepsilon_2) = 2a_1 + a_2 - a_3$; the last line in the third is empty because $a_3(2 \to 3) = 0$.

3.4 Action on $U\varepsilon_2$

$\varepsilon_2\sigma_2\varepsilon_2$:

	a_1	a_2	a_3
a_1	-1		
a_2			1
a_3		1	

$\varepsilon_2\tau\varepsilon_2$:

	a_1	a_2	a_3
a_1	1		-1
a_2	2	1	-1
a_3			1

$(2 \to 3)$:

	a_4	a_5	a_6	a_7	a_8	a_9
a_1			1			-1
a_2	-3	1		2		
a_3						

3.5 Action on $U\varepsilon_3$

$\varepsilon_3\sigma_2\varepsilon_3$:

	a_4	a_5	a_6	a_7	a_8	a_9
a_4		-3			2	
a_5	-3			2		
a_6			-3			2
a_7		-4			3	
a_8	-4			3		
a_9			-4			3

$\varepsilon_3\sigma_3\varepsilon_3$:

	a_4	a_5	a_6	a_7	a_8	a_9
a_4		1				
a_5			1			
a_6	1					
a_7					1	
a_8						1
a_9				1		

$\varepsilon_3\tau\varepsilon_3$:

	a_4	a_5	a_6	a_7	a_8	a_9
a_4	1	2			-2	
a_5		1				
a_6			1			
a_7		4		1	-3	
a_8					1	
a_9						1

$(3 \to 2)$:

	a_1	a_2	a_3
a_4		-1	
a_5		3	
a_6	-2		
a_7			
a_8		4	
a_9	-4		

$(3 \to 4)$:

	a_{10}	a_{11}	a_{12}
a_4	1	1	-1
a_5			
a_6			
a_7	1	1	-2
a_8			
a_9			

3.6 Action on $U\varepsilon_4$

$\varepsilon_4\sigma_2\varepsilon_4$:

	a_{10}	a_{11}	a_{12}
a_{10}		1	
a_{11}	1		
a_{12}			1

$\varepsilon_4\sigma_4\varepsilon_4$:

	a_{10}	a_{11}	a_{12}
a_{10}			-1
a_{11}		-1	
a_{12}	1		

$\varepsilon_4\tau\varepsilon_4$:

	a_{10}	a_{11}	a_{12}
a_{10}	1		
a_{11}		1	
a_{12}			1

$(4 \to 3)$:

	a_4	a_5	a_6	a_7	a_8	a_9
a_{10}	2			-1		
a_{11}	2			-1		
a_{12}	2			-2		

3.7 Action on $V\varepsilon_3$

$\varepsilon_3\sigma_2\varepsilon_3$:

	b_7	b_8	b_9
b_7		-1	
b_8	-1		
b_9			-1

$\varepsilon_3\sigma_3\varepsilon_3$:

	b_7	b_8	b_9
b_7		1	
b_8			1
b_9	1		

$\varepsilon_3\tau\varepsilon_3$:

	b_7	b_8	b_9
b_7	1	1	
b_8		1	
b_9			1

$(3 \to 4)$:

	b_{10}	b_{11}	b_{12}
b_7	-1	1	
b_8			
b_9			

3.8 Action on $V\varepsilon_4$

$\varepsilon_4\sigma_2\varepsilon_4$:

	b_{10}	b_{11}	b_{12}
b_{10}		-1	
b_{11}	-1		
b_{12}			-1

$\varepsilon_4\sigma_4\varepsilon_4$:

	b_{10}	b_{11}	b_{12}
b_{10}			1
b_{11}		1	
b_{12}	-1		

$\varepsilon_4 \tau \varepsilon_4$:

	b_{10}	b_{11}	b_{12}
b_{10}	1		
b_{11}		1	
b_{12}			1

$(4 \to 3)$:

	b_7	b_8	b_9
b_{10}	-1		
b_{11}	1		
b_{12}			

4.

IDEMPOTENTS AND FURTHER REDUCTION

In the previous section we commenced the study of the $\mathbb{Z}_2G$-module W and, in particular, of its submodules U and V. The first round of reductions simplified the context to $\varepsilon\mathbb{Z}_2G\varepsilon$, $W\varepsilon$, $U\varepsilon$, $V\varepsilon$. The union of the $\mathbb{Z}_2$-bases we chose for $U\varepsilon$ and $V\varepsilon$ is a basis for $U\varepsilon \oplus V\varepsilon$; we know explicitly how a generating set of $\varepsilon\mathbb{Z}_2G\varepsilon$ acts on this basis.

In order to be able to get further, we must cut down our ring to that which is actually acting on our modules. Regard $\mathrm{End}_{\mathbb{Z}_2}U\varepsilon \oplus \mathrm{End}_{\mathbb{Z}_2}V\varepsilon$ naturally embedded in $\mathrm{End}_{\mathbb{Z}_2}U\varepsilon \oplus V\varepsilon$, and let S denote the homomorphic image of $\varepsilon\mathbb{Z}_2G\varepsilon$ in $\mathrm{End}_{\mathbb{Z}_2}U\varepsilon \oplus \mathrm{End}_{\mathbb{Z}_2}V\varepsilon$ (so S consists of the endomorphisms of $U\varepsilon \oplus V\varepsilon$ which give the action of $\varepsilon\mathbb{Z}_2G\varepsilon$). The information gathered so far provides us with a generating set for S. The aim of this section is, in effect, to understand precisely which elements of $\mathrm{End}_{\mathbb{Z}_2}U\varepsilon \oplus \mathrm{End}_{\mathbb{Z}_2}V\varepsilon$ lie in S. We forget $\varepsilon\mathbb{Z}_2G\varepsilon$ for the time being, transferring the names of its elements to the corresponding elements of S. Thus, for instance, we have $\varepsilon_1 = 0$ and $\varepsilon = 1$ in S, for this is how ε_1 and ε act on $U\varepsilon \oplus V\varepsilon$.

The decisive step is that we can pick 12 pairwise orthogonal idempotents $\xi_1, \ldots, \xi_{12}$ in S, with sum 1, none of which annihilates $U\varepsilon$ and only (the first) six of which annihilate $V\varepsilon$. This is a largely *ad hoc* move, but the mere fact that it succeeds, no matter how, has implications which are perhaps easier to understand before the details of

choice are added to the picture. Indeed, $U\varepsilon = \oplus U\varepsilon\xi_i$ is then a direct sum of $\mathbb{Z}_2$-modules, with 12 nonzero summands; as $U\varepsilon$ is $\mathbb{Z}_2$-free of rank 12, it follows that $U\varepsilon\xi_i \cong \mathbb{Z}_2$ for each i. Hence $U\varepsilon\xi_i = \mathbb{Z}_2 c_i$ for suitable elements c_i of $U\varepsilon$, and these elements form a new basis for $U\varepsilon$. We identify $\mathrm{End}_{\mathbb{Z}_2} U\varepsilon$ with $\mathrm{Mat}(12, \mathbb{Z}_2)$ according to this basis. Similarly, $V\varepsilon = \oplus V\varepsilon\xi_i$ with

$$V\varepsilon\xi_i = \begin{cases} 0 & \text{if } 1 \le i \le 6, \\ \mathbb{Z}_2 d_i & \text{if } 7 \le i \le 12, \end{cases}$$

and $\mathrm{End}_{\mathbb{Z}_2} V\varepsilon$ is identified with $\mathrm{Mat}(6, \mathbb{Z}_2)$ according to the new basis $d_7, \ldots, d_{12}$. To match labels, we write the elementary matrices of this $\mathrm{Mat}(6, \mathbb{Z}_2)$ as $e_6(i, j)$ with $i, j \in \{7, \ldots, 12\}$. By the choice of $c_1, \ldots, c_{12}, d_7, \ldots, d_{12}$,

4.1
$$\xi_i = \begin{cases} e_{12}(i, i) & \text{if } 1 \le i \le 6, \\ e_{12}(i, i) \oplus e_6(i, i) & \text{if } 7 \le i \le 12. \end{cases}$$

In the second major move we show that the elements $e_{12}(i, j)$ with $i, j \in \{2, \ldots, 5\}$ and the $e_{12}(i, j) \oplus e_6(i, j)$ with $i, j \in \{7, \ldots, 11\}$ all lie in S. These elements, together with the ξ_i, clearly satisfy multiplicative relations like 2.3, and so the element e of S defined by

$$e = \xi_1 + \xi_2 + \xi_6 + \xi_7 + \xi_{12}$$

is an idempotent with $SeS = S$. Thus we can apply 2.1 and 2.2 once more. This second reduction will cut down our task considerably.

Before embarking on this program, let us sketch how all this relates to the results stated in the introduction for $\mathbb{Z}_2G/\mathrm{Ann}\ V$ and other similar rings. Let S_V stand for the projection of S into $\mathrm{End}_{\mathbb{Z}_2} V\varepsilon$ (thus S_V consists of the second components of the elements of S when they are decomposed according to $S \leq \mathrm{End}_{\mathbb{Z}_2} U\varepsilon \oplus \mathrm{End}_{\mathbb{Z}_2} V\varepsilon$). We know from 4.1 that S_V contains all the $e_6(i, i)$; therefore

$$S_V = \oplus\oplus e_6(i, i)S_V e_6(j, j) \quad \text{as } \mathbb{Z}_2\text{-module},$$

and each $e_6(i, i)S_V e_6(j, j)$ is either 0 or $2^{d(i,j)}\mathbb{Z}_2 e_6(i, j)$ for some nonnegative integer $d(i, j)$. The natural way to describe S_V is then to give the table of the $d(i, j)$ [where one would put $d(i, j) = \infty$ if the corresponding component were 0]. The second major move described above means that we have $d(i, j) = 0$ except perhaps when one and only one of i, j is 12 . Ignoring the origin of the $d(i, j)$ for the moment, one notes that $\oplus\oplus 2^{d(i,j)}\mathbb{Z}_2 e_6(i, j)$ is a subring of $\mathrm{Mat}(6, \mathbb{Z}_2)$ if and only if

4.2 $$d(i, j) + d(j, k) \geq d(i, k) \quad \text{for all } i, j, k :$$

thus our $d(i, j)$ must satisfy these inequalities. In particular, as all but 10 of our $d(i, j)$ are already known to be 0 , these inequalities imply that

$$d(7, 12) = d(8, 12) = \ldots = d(11, 12) ,$$

$$d(12, 7) = d(12, 8) = \ldots = d(12, 11) .$$

We claim these $d(i, j)$ all equal 1. To verify this, one checks that with this choice $\oplus\oplus 2^{d(i,j)}\mathbb{Z}_2 e_6(i, j)$ is a ring, as 4.2 is satisfied. Then one checks that the matrices representing the action of the generators of S on $V\varepsilon$ all lie in this ring, so S_V lies in this ring. Finally, one shows that, say, $2e_6(11, 12)$ and $2e_6(12, 10)$ are in S_V, so no smaller ring described by such parameters can contain S_V. (As we take advantage of the reduction using e, we do not actually proceed like this, but in effect we have to carry out all these checks.)

The repetitious, or "blocked", nature of the table of the $d(i, j)$ shows that S_V can be viewed as a ring of "blocked matrices" over the ring $\mathbb{Z}_2 e_2(1, 1) \oplus 2\mathbb{Z}_2 e_2(1, 2) \oplus 2\mathbb{Z}_2 e_2(2, 1) \oplus \mathbb{Z}_2 e_2(2, 2)$. To say that S_V is Morita equivalent to this ring, is true, but is saying rather less: Morita equivalence is defined in terms of categories of modules, and so suppresses individual elements of the rings and modules concerned. (Our reference on Morita equivalence is Anderson and Fuller [1].) Similarly, under the hypotheses of 2.1 one could say that R and $\varepsilon R\varepsilon$ are Morita equivalent, but this would be inadequate for our purposes: we want to keep track of generating sets of submodules, so we also need 2.2. We used "Morita equivalence" in the introduction only to enable us to communicate at least a little about our findings without going through an interminable sequence of definitions; we shall say no more about those weak versions. One could take time to make precise the meaning of "blocked matrices" above, and to show that the previous round of reductions was also of this nature; back-tracking through the detail, one would find the justification of the description we gave in the introduction for $\mathbb{Z}_2 G/\mathrm{Ann}\ V$ as a ring of certain 15×15 matrices. We leave this to the reader who is interested in what, for us here, is a side issue: the matter at hand is complex enough without

it.

Our first detailed task is to produce the ξ_i . A little shorthand will help: for a polynomial f over $\mathbb{Z}_2$ and $\varphi, \alpha, \beta, \ldots \in S$, we shall write $f(\varphi\alpha\varphi, \varphi\beta\varphi, \ldots)$ as $\varphi[\![f(\alpha, \beta, \ldots)]\!]\varphi$. (For instance, $\varepsilon_3[\![\sigma_2\tau+1]\!]\varepsilon_3$ means $(\varepsilon_3\sigma_2\varepsilon_3)(\varepsilon_3\tau\varepsilon_3) + \varepsilon_3$.) With this convention, let

$$\zeta = \varepsilon_2[\![\sigma_2\mu_{-1}\tau]\!]\varepsilon_2 ,$$

$$\eta = \varepsilon_3\Big[\!\Big[\Big(1+(\sigma_2+\tau-1)\sigma_3^2\Big)(1-\tau)\sigma_2\Big]\!\Big]\varepsilon_3 .$$

The last paragraph of Section 2 shows how ζ leads to

$$\xi_1 = \tfrac{1}{3}\varepsilon_2[\![1+\zeta+\zeta^2]\!]\varepsilon_2 ,$$

$$\xi_2 = \tfrac{1}{3}\varepsilon_2\Big[\!\Big[1-\zeta-\sigma_2\zeta+\sigma_2\zeta^2\Big]\!\Big]\varepsilon_2 ,$$

$$\xi_3 = \tfrac{1}{3}\varepsilon_2\Big[\!\Big[1-\zeta^2+\sigma_2\zeta-\sigma_2\zeta^2\Big]\!\Big]\varepsilon_2 :$$

three pairwise orthogonal idempotents with sum ε_2 . Next, use the tables at the end of Section 3 to calculate that, on the (old) bases of $U\varepsilon_3$ and $V\varepsilon_3$, η acts as $\mathrm{diag}(0, 0, 0, 1, 0, 0)$ and $\mathrm{diag}(1, 0, 0)$, respectively; and that therefore ξ_7, ξ_8, ξ_9 chosen as

$$\xi_7 = \eta ,$$

$$\xi_8 = \varepsilon_3\Big[\!\Big[\sigma_3^2\eta\sigma_3\Big]\!\Big]\varepsilon_3 ,$$

$$\xi_9 = \varepsilon_3\Big[\!\Big[\sigma_3\eta\sigma_3^2\Big]\!\Big]\varepsilon_3 ,$$

act on (the old bases of) $U\varepsilon_3$ and $V\varepsilon_3$ as pairwise orthogonal (diagonal) idempotents. Put

$$\xi = \varepsilon_3 - (\xi_7+\xi_8+\xi_9) \ ;$$

note that $\xi\varepsilon_3 = \varepsilon_3\xi = \xi$; ξ annihilates ε_2, ε_4 , and $V\varepsilon$, and acts as diag(1, 1, 1, 0, 0, 0) on $U\varepsilon_3$. One can readily see from those tables that multiplicatively $\frac{1}{3}\xi\sigma_2\xi$ $(= \frac{1}{3}\xi\varepsilon_3\sigma_2\varepsilon_3\xi)$ and $\xi\sigma_3\xi$ $(= \xi\varepsilon_3\sigma_3\varepsilon_3\xi)$ generate another isomorphic copy of the symmetric group S_3 ; hence

$$\xi_4 = \tfrac{1}{3}\xi\left\|\overline{\underline{1-\sigma_3-\tfrac{1}{3}\sigma_2\sigma_3+\tfrac{1}{3}\sigma_2\sigma_3^2}}\right\|\xi \ ,$$

$$\xi_5 = \tfrac{1}{3}\xi\left\|\overline{\underline{1-\sigma_3^2+\tfrac{1}{3}\sigma_2\sigma_3-\tfrac{1}{3}\sigma_2\sigma_3^2}}\right\|\xi \ ,$$

$$\xi_6 = \tfrac{1}{3}\xi\left\|\overline{\underline{1+\sigma_3+\sigma_3^2}}\right\|\xi \ ,$$

define three more pairwise orthogonal idempotents, with sum ξ ; so $\xi_4 + \ldots + \xi_9 = \varepsilon_3$. Finally, put

$$\xi_{10} = \tfrac{1}{3}\varepsilon_4\left\|\overline{\underline{1-\sigma_3-\sigma_2\sigma_3+\sigma_2\sigma_3^2}}\right\|\varepsilon_4 \ ,$$

$$\xi_{11} = \tfrac{1}{3}\varepsilon_4\left\|\overline{\underline{1-\sigma_3^2+\sigma_2\sigma_3-\sigma_2\sigma_3^2}}\right\|\varepsilon_4 \ ,$$

$$\xi_{12} = \tfrac{1}{3}\varepsilon_4\left\|\overline{\underline{1+\sigma_3+\sigma_3^2}}\right\|\varepsilon_4 \ :$$

we have already seen in the second last paragraph of Section 2 that these are pairwise orthogonal idempotents with sum ε_4 . As $\varepsilon_2 + \varepsilon_3 + \varepsilon_4 = \varepsilon = 1$ in S , all this combined proves the following.

4.3 LEMMA. *The* $\xi_1, \ldots, \xi_{12}$ *so defined are pairwise orthogonal idempotents with sum* 1 *in* S .

The next point is to show that none of the $U\varepsilon\xi_i$ $(1 \le i \le 12)$ and $V\varepsilon\xi_j$ $(7 \le j \le 12)$ is 0 , and indeed to choose elements $c_1, \ldots, c_{12}$,

$d_7, \ldots, d_{12}$ such that these form a basis of $U\varepsilon \oplus V\varepsilon$ with $c_i\xi_i = c_i$, $d_j\xi_j = d_j$. The way we chose the ξ_i suggests how to do this. Instead of taking the reader through the detail of how one implements that suggestion, we give the end result in a form which also has further uses. We shall write down below 12×12 matrices α, α' and 6×6 matrices β, β' over $\mathbb{Z}$, leaving to the reader the tedious but straightforward verification of the following.

4.4 LEMMA. *For the elements* $c_1, \ldots, d_{12}$ *defined by*

$$c_i = \sum_{k=1}^{12} \alpha_{ik} a_k \quad (1 \le i \le 12),$$

$$d_j = \sum_{k=7}^{12} \beta_{jk} b_k \quad (7 \le j \le 12),$$

$c_i\xi_i = c_i$ *and* $d_j\xi_j = d_j$; *while* $\frac{1}{3}\alpha\alpha'$ *and* $\frac{1}{3}\beta\beta'$ *are identity matrices.*

It then follows that $\alpha^{-1} = \frac{1}{3}\alpha' \in \mathrm{Mat}(12, \mathbb{Z}_2)$ and $\beta^{-1} = \frac{1}{3}\beta' \in \mathrm{Mat}(6, \mathbb{Z}_2)$, so the c_i, d_j do form a basis of the required kind. Moreover, these matrices can be used to calculate the matrix form of the generators of S with respect to this new basis of $U\varepsilon \oplus V\varepsilon$: an unavoidable exercise which must be performed next. The calculations are facilitated by the fact that both the old and the new bases are naturally grouped into lots of 3 (successive) basis elements; the old matrices listed at the end of the previous section contained only zeros outside certain 3×3 blocks (indeed, we only wrote down the nonvanishing blocks), and the conversion matrices $\alpha, \alpha^{-1}, \beta, \beta^{-1}$ contain only zeros outside their diagonal 3×3 blocks. Thus it is convenient to write

$$\alpha = \mathrm{diag}\left(\begin{pmatrix} 1 & 1 & -1 \\ 2 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ 1 & 1 & 1 \end{pmatrix}\right),$$

$$\alpha' = \mathrm{diag}\left(\begin{pmatrix} -1 & 1 & -1 \\ 2 & 1 & 2 \\ -2 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 1 \\ -2 & -1 & 1 \\ 1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ -1 & -1 & 1 \end{pmatrix}\right),$$

$$\beta = \mathrm{diag}\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}\right),$$

$$\beta' = \mathrm{diag}\left(\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} -1 & -2 & 1 \\ 2 & 1 & 1 \\ -1 & 1 & 1 \end{pmatrix}\right).$$

Notice that while previously we could suppress the obvious diagonal matrices representing the $\varepsilon_i \mu_\kappa \varepsilon_i$ on the old bases, these elements no longer act diagonally, so now we must give their matrix forms explicitly. The format of the following tables follows the precedent established at the end of Section 3. Where a matrix would have fractional entries, for simplicity we write down a multiple (by a unit of $\mathbb{Z}_2$).

4.5 Action on $U\varepsilon_2$

$\varepsilon_2\sigma_2\varepsilon_2$:

	c_1	c_2	c_3
c_1	-1		
c_2			1
c_3		1	

$3\varepsilon_2\tau\varepsilon_2$:

	c_1	c_2	c_3
c_1	5	-2	-4
c_2	4	-1	-5
c_3	-4	4	5

$3\varepsilon_2\mu_\kappa\varepsilon_2$:

	c_1	c_2	c_3
c_1	$\kappa(2\kappa^2-\kappa+2)$	$\kappa(\kappa-1)(\kappa+2)$	$\kappa(\kappa-1)(2\kappa+1)$
c_2	$2\kappa^2(\kappa-1)$	$\kappa^2(\kappa+2)$	$2\kappa^2(\kappa-1)$
c_3	$2\kappa(\kappa-1)$	$-2\kappa(\kappa-1)$	$\kappa(2\kappa+1)$

$3(2 \to 3)$:

	c_4	c_5	c_6	c_7	c_8	c_9
c_1	-4	-8	-1	6	0	-3
c_2	-3	-9	0	6	0	-6
c_3	-2	2	-2	0	0	6

4.6 Action on $U\varepsilon_3$

$3\varepsilon_3\sigma_2\varepsilon_3$:

	c_4	c_5	c_6	c_7	c_8	c_9
c_4		9		-6		6
c_5	9				6	-6
c_6			-9	6	6	6
c_7	8	4	-4		9	
c_8	-4	-8	-4	9		
c_9	-4	4	-4			9

$\varepsilon_3\sigma_3\varepsilon_3$:

	c_4	c_5	c_6	c_7	c_8	c_9
c_4		1				
c_5	-1	-1				
c_6			1			
c_7					1	
c_8						1
c_9				1		

$3\varepsilon_3\mu_\kappa\varepsilon_3$:

	c_4	c_5	c_6	c_7	c_8	c_9
c_4	3κ					
c_5	$\kappa(\kappa-1)$	$\kappa(2\kappa+1)$	$\kappa(\kappa-1)$			
c_6	$\kappa(\kappa-1)$	$2\kappa(\kappa-1)$	$\kappa(\kappa+2)$			
c_7				$3\kappa^2$		
c_8					3κ	
c_9						3κ

$3\varepsilon_3\tau\varepsilon_3$:

	c_4	c_5	c_6	c_7	c_8	c_9
c_4	3					
c_5	-4	1	2		-6	
c_6	-4	-2	5		-6	
c_7	-8	-4	4	3	-9	
c_8					3	
c_9						3

$3(3 \to 2)$:

	c_1	c_2	c_3
c_4	-4	-5	-4
c_5	-4	1	-4
c_6	6		6
c_7			
c_8	8	4	8
c_9	4	-4	4

$3(3 \to 4)$:

	c_{10}	c_{11}	c_{12}
c_4			
c_5	2	2	1
c_6	2	2	1
c_7	3	3	
c_8			
c_9			

4.7 Action on $U\varepsilon_4$

$\varepsilon_4\sigma_2\varepsilon_4$:

	c_{10}	c_{11}	c_{12}
c_{10}		1	
c_{11}	1		
c_{12}			1

$3\varepsilon_4\sigma_4\varepsilon_4$:

	c_{10}	c_{11}	c_{12}
c_{10}	1	3	-2
c_{11}	-2	-3	-2
c_{12}	2	0	-1

$\varepsilon_4\mu_\kappa\varepsilon_4$:

	c_{10}	c_{11}	c_{12}
c_{10}	κ		
c_{11}		κ	
c_{12}			κ

$\varepsilon_4\tau\varepsilon_4$:

	c_{10}	c_{11}	c_{12}
c_{10}	1		
c_{11}		1	
c_{12}			1

		c_4	c_5	c_6	c_7	c_8	c_9
	c_{10}				1		
$(4 \to 3)$:	c_{11}				1		
	c_{12}	2	4	2	-4		

4.8 Action on $V\varepsilon_3$

		d_7	d_8	d_9
	d_7		-1	
$\varepsilon_3\sigma_2\varepsilon_3$:	d_8	-1		
	d_9			-1

		d_7	d_8	d_9
	d_7		1	
$\varepsilon_3\sigma_3\varepsilon_3$:	d_8			1
	d_9	1		

		d_7	d_8	d_9
	d_7	κ^2		
$\varepsilon_3\mu_\kappa\varepsilon_3$:	d_8		κ	
	d_9			κ

		d_7	d_8	d_9
	d_7	1	1	
$\varepsilon_3\tau\varepsilon_3$:	d_8		1	
	d_9			1

		d_{10}	d_{11}	d_{12}
	d_7	1	1	
$(3 \to 4)$:	d_8			
	d_9			

4.9 Action on $V\varepsilon_4$

		d_{10}	d_{11}	d_{12}
	d_{10}		1	
$\varepsilon_4\sigma_2\varepsilon_4$:	d_{11}	1		
	d_{12}			-1

		d_{10}	d_{11}	d_{12}
	d_{10}	1	-1	2
$3\varepsilon_4\sigma_4\varepsilon_4$:	d_{11}	2	1	-2
	d_{12}	2	4	1

		d_{10}	d_{11}	d_{12}
	d_{10}	κ		
$\varepsilon_4\mu_\kappa\varepsilon_4$:	d_{11}		κ	
	d_{12}			κ

		d_{10}	d_{11}	d_{12}
	d_{10}	1		
$\varepsilon_4\tau\varepsilon_4$:	d_{11}		1	
	d_{12}			1

$$
\begin{array}{lccc}
 & d_7 & d_8 & d_9 \\
 & d_{10} & 1 & \\
(4 \to 3) : & d_{11} & 1 & \\
 & d_{12} & &
\end{array}
$$

4.10 LEMMA. *The elements*

$$e_{12}(i, j) \quad \textit{with} \quad i, j \in \{2, \ldots, 5\}$$

and the

$$e_{12}(i, j) \oplus e_6(i, j) \quad \textit{with} \quad i, j \in \{7, \ldots, 11\}$$

are all contained in S .

Proof. Note that $e_{12}(2, 3) = \xi_2\varepsilon_2\sigma_2\varepsilon_2\xi_3 \in S$, simply because the $(2, 3)$ entry in the new matrix form of $\varepsilon_2\sigma_2\varepsilon_2$ on $U\varepsilon$ is 1 and $\varepsilon_2\sigma_2\varepsilon_2$ annihilates $V\varepsilon$. Also, $e_{12}(7, 8) \oplus e_6(7, 8) = \xi_7\varepsilon_3\sigma_3\varepsilon_3\xi_8 \in S$ because the $(7, 8)$ entries of the new matrices of $\varepsilon_3\sigma_3\varepsilon_3$ on $U\varepsilon$ and $V\varepsilon$ are both 1 . The inspection of

the	$(3, 2)$	entry for	$\varepsilon_2\sigma_2\varepsilon_2$,
the	$(2, 4)$ and $(2, 5)$	entry for	$(2 \to 3)$,
the	$(4, 2)$ and $(5, 2)$	entry for	$(3 \to 2)$,
the	$(8, 9)$ and $(9, 7)$	entries for	$\varepsilon_3\sigma_3\varepsilon_3$,
the	$(7, 10)$ and $(7, 11)$	entries for	$(3 \to 4)$, and
the	$(10, 7)$ and $(11, 7)$	entries for	$(4 \to 3)$

show that the $e_{12}(i, j)$ and the $e_{12}(i, j) \oplus e_6(i, j)$ with (i, j) already considered are all in S . The other elements mentioned in the

lemma are products of these (by the multiplication rule of elementary matrices), so they are also in S . //

The elements of S which we know from 4.1 and 4.10 clearly span (over $\mathbb{Z}_2$) a direct sum of (isomorphic copies of) full matrix rings of degrees 1, 4, 1, 5, 1 . Formally, define

$$i' = \begin{cases} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{cases} \quad \text{and} \quad i^* = \begin{cases} 1 & \text{if } i = 1 , \\ 2 & \text{if } 2 \le i \le 5 , \\ 6 & \text{if } i = 6 , \\ 7 & \text{if } 7 \le i \le 11 , \\ 12 & \text{if } i = 12 , \end{cases}$$

and rename

$$\left.\begin{array}{l} e_{12}(i, j) \\ \\ \\ e_{12}(i, j) \oplus e_6(i, j) \end{array}\right\} = \varepsilon^{i'}_{i+1-i^*, j+1-j^*} \qquad \begin{array}{l} \text{if } i' = j' \le 3 , \\ \\ \\ \text{if } i' = j' \ge 4 . \end{array}$$

These elements satisfy 2.3 and 2.4, so it follows that

$$e = \xi_1 + \xi_2 + \xi_6 + \xi_7 + \xi_{12}$$

defines an idempotent e with $SeS = S$, and 2.1, 2.2, 2.6 become applicable. Note that the elements $\varepsilon^{k}_{1\ell}$ and ε^{m}_{n1} relevant in 2.6 now come from the positions (i^*, i) and (j, j^*) , respectively.

Thus we can shift our attention to eSe-submodules of $(U\varepsilon \oplus V\varepsilon)e$. Let $u_1 = c_1$, $u_2 = c_2$, $u_3 = c_6$, $u_4 = c_7$, $u_5 = c_{12}$, $v_4 = d_7$, $v_5 = d_{12}$: then $\{u_1, \ldots, u_5\}$ and $\{v_4, v_5\}$ are $\mathbb{Z}_2$-bases of $(U\varepsilon)e$ and $(V\varepsilon)e$, respectively. We identify $\mathrm{End}_{\mathbb{Z}_2}(U\varepsilon)e \oplus \mathrm{End}_{\mathbb{Z}_2}(V\varepsilon)e$ with

$\mathrm{Mat}(5, \mathbb{Z}_2) \oplus \mathrm{Mat}(2, \mathbb{Z}_2)$ according to these bases, and consider this direct sum naturally embedded in $\mathrm{End}_{\mathbb{Z}_2}(U\varepsilon \oplus V\varepsilon)e$ which in turn is identified with $\mathrm{Mat}(7, \mathbb{Z}_2)$.

Let T stand for the image of eSe , under restriction to $(U\varepsilon \oplus V\varepsilon)e$, in $\mathrm{Mat}(5, \mathbb{Z}_2) \oplus \mathrm{Mat}(2, \mathbb{Z}_2)$. This change from eSe to T is essentially a notational matter: if an element of eSe is written as $\gamma \oplus \delta$ according to $eSe \leq S \leq \mathrm{Mat}(12, \mathbb{Z}_2) \oplus \mathrm{Mat}(6, \mathbb{Z}_2)$, then the entries $\gamma(i, j)$ of γ vanish unless $i, j \in \{1, 2, 6, 7, 12\}$, and similarly $\delta(i, j) = 0$ unless $i, j \in \{7, 12\}$; to obtain the corresponding element of T , we simply omit the rows and columns which *must* vanish *because* we started with an element of eSe . With this final shift of view, our task becomes the study of the T-submodules of $(U\varepsilon \oplus V\varepsilon)e$.

The main result of this section tells us exactly which elements $\alpha \oplus \beta$ of $\mathrm{Mat}(5, \mathbb{Z}_2) \oplus \mathrm{Mat}(2, \mathbb{Z}_2)$ lie in T . To be able to state it, we shall need the matrix

$$a = (a(i, j)) = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 2 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 \end{bmatrix} .$$

Let T' be the set of all those $\alpha \oplus \beta$ which satisfy the following conditions:

$\alpha(i, j) \in 2^{a(i,j)}\mathbb{Z}_2$ for all i, j in $\{1, \ldots, 5\}$;

$\beta(i, j) \equiv \alpha(i, j) \bmod 4$ for $(i, j) \in \{(4, 4), (4, 5), (5, 4)\}$,

$\beta(5, 5) \equiv \alpha(5, 5) \bmod 2$.

4.11 THEOREM. $T = T'$.

Proof. It is straightforward to verify that T' is a subalgebra of $\mathrm{Mat}(5, \mathbb{Z}_2) \oplus \mathrm{Mat}(2, \mathbb{Z}_2)$. Thus in order to prove that $T \leq T'$, it is sufficient to show that T' contains the generating set of T obtained by 2.6 from the known generating set of S . To see what this involves, let us consider any generator of S in the form $\gamma \oplus \delta$ (with $\gamma \in \mathrm{Mat}(12, \mathbb{Z}_2)$ and $\delta \in \mathrm{Mat}(6, \mathbb{Z}_2)$). As we have already remarked, the generators of eSe arise by premultiplying $\gamma \oplus \delta$ by an $e_{12}(i^*, i)$ or $e_{12}(i^*, i) \oplus e_6(i^*, i)$ [with $i' \leq 3$ or $i' \geq 4$, respectively), and postmultiplying the product by an $e_{12}(j, j^*)$ or $e_{12}(j, j^*) \oplus e_6(j, j^*)$ [with $j' \leq 3$ or $j' \geq 4$, respectively]. So these generators of eSe are the

$$e_{12}(i^*, i)\gamma e_{12}(j, j^*) \text{ with } i' \leq 3 \text{ or } j' \leq 3$$

and the

$$e_{12}(i^*, i)\gamma e_{12}(j, j^*) \oplus e_6(i^*, i)\delta e_6(j^*, j) \text{ with } i' \geq 4 \text{ and } j' \geq 4 .$$

Note that

$$e_{12}(i^*, i)\gamma e_{12}(j, j^*) = \gamma(i, j)e_{12}(i^*, j^*)$$

and

$$e_6(i^*, i)\delta e_6(j, j^*) = \delta(i, j)e_6(i^*, j^*) .$$

Upon restriction to $(U\varepsilon \oplus V\varepsilon)e$, these generators of eSe become the elements

$$\gamma(i, j)e_5(i', j') , \qquad i' \leq 3 \text{ or } j' \leq 3 ,$$

$$\gamma(i, j)e_5(i', j') \oplus \delta(i, j)e_2(i', j') , \qquad i' \geq 4 \text{ and } j' \geq 4$$

of T ; as $\gamma \oplus \delta$ ranges through a generating set of S , these elements build a generating set for T . So $T \leq T'$ will follow if

$$\gamma(i, j) \in 2^{a(i',j')}\mathbb{Z}_2 \quad \text{for all } i, j \text{ in } \{1, \ldots, 12\} ,$$

$$\delta(i, j) \equiv \gamma(i, j) \bmod 4 \quad \text{when } (i', j') \in \{(4, 4), (4, 5), (5, 4)\} ,$$

$$\delta(12, 12) \equiv \gamma(12, 12) \bmod 2 ,$$

for each element $\gamma \oplus \delta$ of our generating set of S . To verify this, one must inspect almost every entry in the tables 4.5-4.9; the only exceptions being the (i, j) entries with $a(i', j') = 0$ and $i' \leq 3$ or $j' \leq 3$.

For the proof of the converse inclusion, $T' \leq T$, we use that checking on $\gamma(i, j)$ in the tables shows that $2^{a(i',j')}e_5(i', j') \in T$, for

$\gamma \oplus \delta$	(i, j)	(i', j')
$\varepsilon_2\tau\varepsilon_2$	(1, 2)	(1, 2)
(2 → 3)	(1, 6)	(1, 3)
(2 → 3)	(1, 9)	(1, 4)
$\varepsilon_2\tau\varepsilon_2$	(2, 1)	(2, 1)
(2 → 3)	(3, 6)	(2, 3)
(2 → 3)	(2, 7)	(2, 4)
(3 → 4)	(5, 12)	(2, 5)
(3 → 2)	(6, 1)	(3, 1)
(3 → 2)	(6, 3)	(3, 2)
$\varepsilon_3\sigma_2\varepsilon_3$	(6, 7)	(3, 4)
(3 → 4)	(6, 12)	(3, 5)
(3 → 2)	(9, 1)	(4, 1)
(3 → 2)	(8, 2)	(4, 2)
$\varepsilon_3\sigma_2\varepsilon_3$	(7, 6)	(4, 3)
(4 → 3)	(12, 4)	(5, 2)
(4 → 3)	(12, 6)	(5, 3)

Of course, $\xi_i \in S$ yields that $e_5(1, 1), e_5(2, 2), e_5(3, 3)$ are also in T. As $a(1, 3) + a(3, 5) = a(1, 5)$ and $a(5, 3) + a(3, 1) = a(5, 1)$, we conclude that $2^{a(i,j)}e_5(i, j) \in T$ also for $(i, j) = (1, 5)$ and $(5, 1)$, so by now we know this for all (i, j) with $i \leq 3$ or $j \leq 3$. This leaves us to prove that T contains the subset T'' of T' defined by

$$T'' = \{\alpha \oplus \beta \in T' \mid \alpha(i, j) = 0 \text{ if } i \leq 3 \text{ or } j \leq 3\} .$$

Now T'' is easily seen to be spanned over $\mathbb{Z}_2$ by the following elements:

$4e_5(4, 4)$, which lies in T because it is

$$2^{a(4,1)}e_5(4, 1)2^{a(1,4)}e_5(1, 4) ,$$

$4e_5(4, 5)$, which lies in T because it is

$$2^{a(4,1)}e_5(4, 1)2^{a(1,5)}e_5(1, 5) ,$$

$4e_5(5, 4)$, which lies in T because it is

$$2^{a(5,1)}e_5(5, 1)2^{a(1,4)}e_5(1, 4) ,$$

$2e_5(5, 5)$, which lies in T because it is

$$2^{a(5,2)}e_5(5, 2)2^{a(2,5)}e_5(2, 5) ,$$

$e_5(4, 4) \oplus e_2(4, 4)$, which lies in T as the restriction of ξ_7,

$2e_5(4, 5) \oplus 2e_2(4, 5)$, which is seen to lie in T by looking up the $(11, 12)$ entries of $\varepsilon_4\sigma_4\varepsilon_4$,

$2e_5(5, 4) \oplus 2e_2(5, 4)$, which is seen to lie in T by looking up the $(12, 10)$ entries of $\varepsilon_4\sigma_4\varepsilon_4$,

$e_5(5, 5) \oplus e_2(5, 5)$, which lies in T as the restriction of ξ_{12}.

This completes the proof of the theorem.

Let T_U denote the restriction of T to $(U\varepsilon)e$; that is, the set of $\mathrm{Mat}(5, \mathbb{Z}_2)$ components of the elements of T ; similarly, let T_V be the projection of T in $\mathrm{Mat}(2, \mathbb{Z}_2)$.

4.12 COROLLARY.

$$T_U = \left\{\alpha \in \mathrm{Mat}(5, \mathbb{Z}_2) \mid \alpha(i, j) \in 2^{a(i,j)}\mathbb{Z}_2\right\} ,$$

$$T_V = \left\{\beta \in \mathrm{Mat}(2, \mathbb{Z}_2) \mid \beta(i, j) \in 2^{a(i,j)}\mathbb{Z}_2\right\} .$$

Proof. Only the second statement calls for comment. Comparing the moduli of the congruence conditions in the definition of T' with the exponents $a(i, j)$ for $i, j \in \{4, 5\}$, one sees that $\alpha \oplus \beta \in T'$ implies $\beta(i, j) \in 2^{a(i,j)}\mathbb{Z}_2$. Conversely, $2^{a(i,j)}\left(e_5(i, j) \oplus e_2(i, j)\right)$ satisfies the defining conditions of T' whenever $i, j \in \{4, 5\}$. //

5.

SUBMODULES OF U AND V

Corollary 4.12 makes it very easy to see just what T-submodules there are in $U\epsilon e$ and $V\epsilon e$; we devote this section to a detailed discussion of these, before proceeding to more complicated matters.

As T_U contains the diagonal elementary matrices $e_5(i, i)$, each T-submodule of $U\epsilon e$ has a $\mathbb{Z}_2$-basis consisting of scalar multiples of the basis elements u_i of $U\epsilon e$. With the convention that $2^\infty = 0$, we may therefore write each submodule in the form $\oplus\, 2^{u(i)}\mathbb{Z}_2\mathsf{u}_i$ where each $u(i)$ is either ∞ or a nonnegative integer. Since T_U has $\mathbb{Z}_2$-basis $2^{a(i,j)}e_5(i, j)$, such a $\mathbb{Z}_2$-submodule admits T if and only if

5.1 $\qquad u(i) + a(i, j) \geq u(j)$ for all i, j in $\{1, \ldots, 5\}$.

In particular, it follows that if $\oplus\, 2^{u(i)}\mathbb{Z}_2\mathsf{u}_i$ is a T-submodule and one of the $u(i)$ is ∞ then all the $u(i)$ must be ∞ , that is, the submodule is 0 . Also, $\mathsf{u}_iT = \oplus\, 2^{a(i,j)}\mathbb{Z}_2\mathsf{u}_j$. In view of the connection we established by repeated use of 2.1, 2.2 between the T-submodules of $U\epsilon e$ and the $\mathbb{Z}_2G$-submodules of U , we therefore have the following.

5.2 **THEOREM.** *The nonzero $\mathbb{Z}_2G$-submodules of U are in one-to-one correspondence with the (ordered) 5-tuples*

$$\big(u(1), u(2), \ldots, u(5)\big)$$

of nonnegative integers satisfying 5.1; *namely, the submodule of U*

corresponding to such a 5*-tuple is* $\sum 2^{u(i)}\mathfrak{u}_i\mathbb{Z}_2G$. *This submodule contains the submodule corresponding to* $(u'(1), \ldots, u'(5))$ *if and only if* $u(1) \le u'(1), \ldots, u(5) \le u'(5)$. *More generally, the sum and the intersection of these two submodules correspond to the* 5*-tuples*

$$(\min\{u(1), u'(1)\}, \ldots, \min\{u(5), u'(5)\})$$

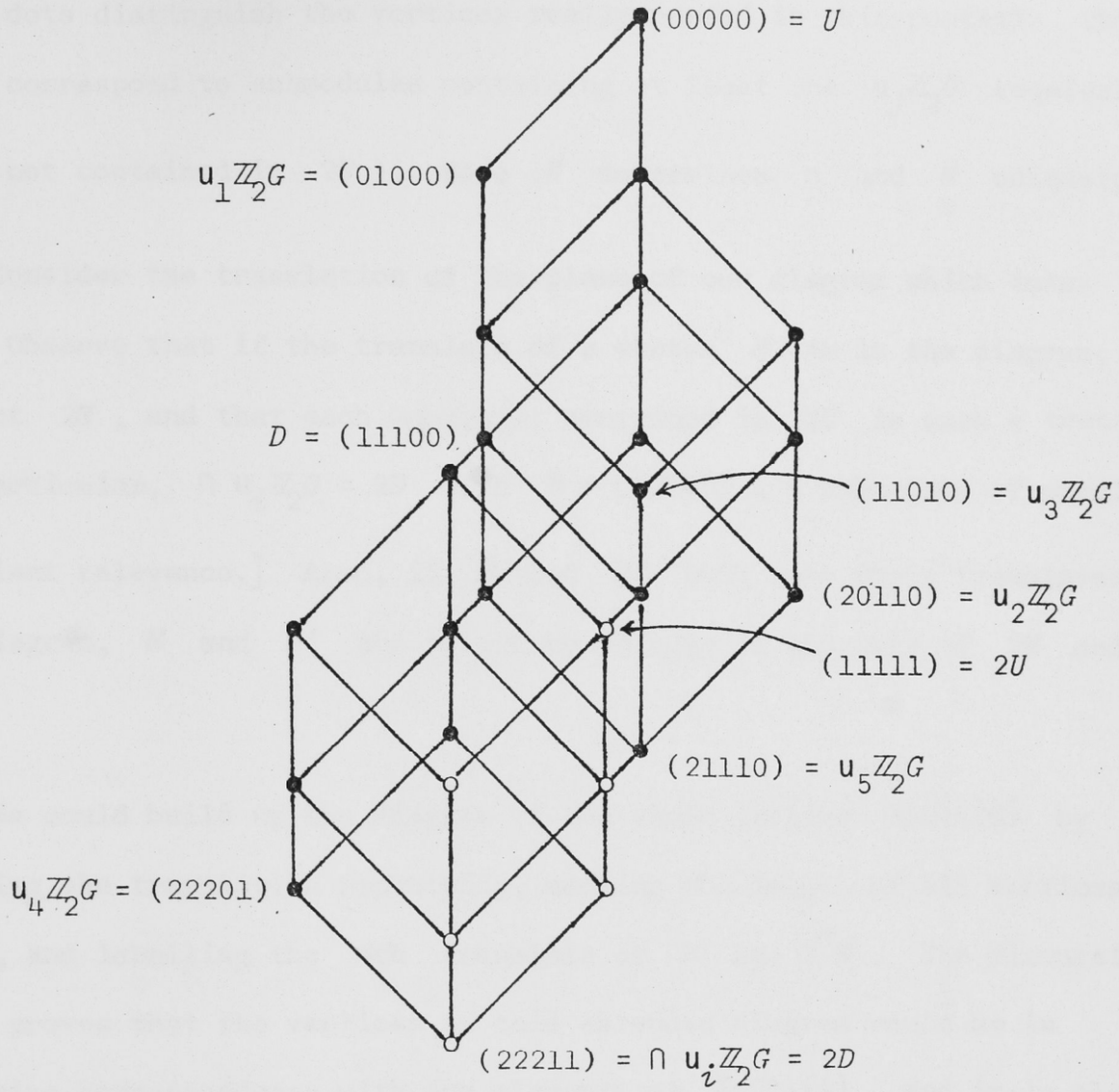
and

$$(\max\{u(1), u'(1)\}, \ldots, \max\{u(5), u'(5)\}) ,$$

respectively. In particular, U *corresponds to* $(0, \ldots, 0)$, *and* $\mathfrak{u}_i\mathbb{Z}_2G$ *to* $(a(i, 1), \ldots, a(i, 5))$.

To visualize just which 5-tuples satisfy 5.1 and how the corresponding submodules relate to each other, we have drawn the diagram of the sublattice of the submodule lattice $S(U)$ of U consisting of the submodules which contain $\cap\, \mathfrak{u}_i\mathbb{Z}_2G$. For the moment, whenever convenient we identify a submodule with the corresponding 5-tuple; the omitted vertex labels of the diagram are readily obtainable by the rules for sums and intersections given in Theorem 5.2.

One helpful formal property of 5.1 is that if $(u(1), \ldots, u(5))$ satisfies it, so does $(u(1)+1, \ldots, u(5)+1)$: thus if the former corresponds to the submodule M , the 5-tuple corresponding to $2M$ is the latter. Similarly, if $0 \ne N \in S(U)$ and $N = (u(1), \ldots, u(5))$, we may take $n = \min\{u(1), \ldots, u(5)\}$, define M as $\sum 2^{u(i)-m}\mathfrak{u}_i\mathbb{Z}_2G$ so $N = 2^nM$, and conclude that $M = (u(1)-n, \ldots, u(5)-n)$. As $u(j) = n$ for some j , for that j we have $u(j) - n = 0$ and hence $M \ge \mathfrak{u}_j\mathbb{Z}_2G \ge \cap\, \mathfrak{u}_i\mathbb{Z}_2G$: thus M is one of the vertices of our diagram.



Submodule lattice of U

Heavy dots distinguish the vertices really needed in this context: those which correspond to submodules containing at least one $u_j\mathbb{Z}_2G$ (equivalently: those not contained in $2U$). Note N determines n and M uniquely.

Consider the translation of the plane of our diagram which takes U to $2U$. Observe that if the translate of a vertex M is in the diagram, it is in fact $2M$, and that each vertex contained in $2U$ is such a translate. [In particular, $\cap\, u_i\mathbb{Z}_2G = 2D$ with $D = (11100)$, a submodule of purely transient relevance.] Also, if M and M' both have their translates in the diagram, M and M' are joined by an edge if and only if $2M$ and $2M'$ are.

We could build up the diagram of the whole lattice $S(U)\backslash\{0\}$ by applying the translation repeatedly, marking the images of all vertices and edges, and labelling the nth translate of M by 2^nM. The discussion above proves that the vertices in this extended diagram would be in bijective correspondence with the elements of $S(U)\backslash\{0\}$, and it is clear that all edges drawn would be justified. The remaining point is that every necessary edge would get drawn this way. To see this, suppose $2^{n'}M'$ is a maximal submodule of 2^nM (where $M \nleq 2U$ and $M' \nleq 2U$). If $n = n'$, our instructions ensure that an edge is drawn joining 2^nM to $2^{n'}M'$. If $n > n'$, then $M' < 2^{n-n'}M \leq 2U$, so this is excluded by our assumptions. Suppose then that $n < n'$. Now $2^{n'-n}M'$ is a maximal submodule of M. We cannot have $2^{n'-n}M' + 2D = M$, for $M \nleq 2U$; on the other hand, $M \nleq 2U$ implies $2D \leq M$: so $2^{n'-n}M'$ must contain $2D$. Thus $2^{n'-n}M'$ and M are both vertices in the diagram we have actually drawn, so there is an edge joining them, and our instructions provide that one will be drawn joining

$2^{n'}M'$ and $2^{n}M$. This establishes that the whole of $S(U)\backslash\{0\}$ can be visualized as indicated.

The submodules of V are understood similarly, the role of 5.1 being taken by

5.3 $\qquad v(i) + a(i, j) \geq v(j)$ for all i, j in $\{4, 5\}$.

Of course, the nontrivial part of 5.3 may be written simply as

5.3' $\qquad v(4) - 1 \leq v(5) \leq v(4) + 1$.

5.4. THEOREM. *The nonzero $\mathbb{Z}_2G$-submodules of V are in one-to-one correspondence with the ordered pairs*

$$\big(v(4),\ v(5)\big)$$

of nonnegative integers satisfying 5.3; *namely, the submodule of V corresponding to such a pair is $2^{v(4)}\vee_4 \mathbb{Z}_2G + 2^{v(5)}\vee_5 \mathbb{Z}_2G$. This submodule contains the submodule corresponding to $\big(v'(4),\ v'(5)\big)$ if and only if $v(4) \leq v'(4)$ and $v(5) \leq v'(5)$. More generally, the sum and the intersection of these two submodules correspond to*

$$\big(\min\{v(4),\ v'(4)\},\ \min\{v(5),\ v'(5)\}\big)$$

and

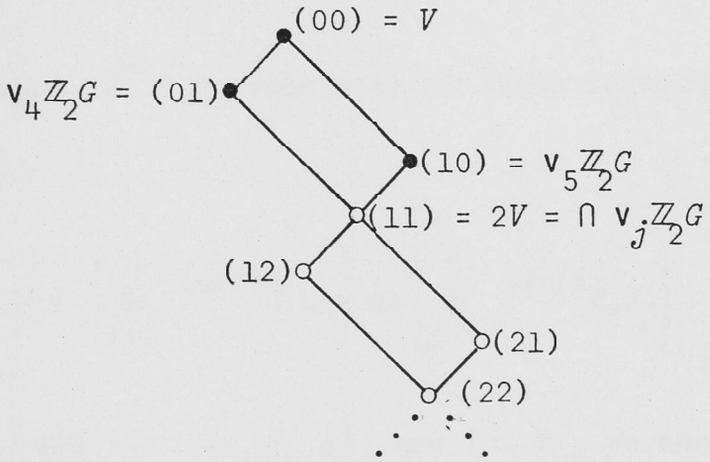
$$\big(\max\{v(4),\ v'(4)\},\ \max\{v(4),\ v'(4)\}\big)\ ,$$

respectively. In particular, V corresponds to $(0, 0)$, and $\vee_i \mathbb{Z}_2G$ to $\big(a(i, 4),\ a(i, 5)\big)$.

The reason we put the theorem in this elaborate form is that later on we have to combine it with 5.2, but of course one can express it much more

concisely: the nonzero $\mathbb{Z}_2G$-submodules of V are just the 2^iV, $2^jv_4\mathbb{Z}_2G$, $2^kv_5\mathbb{Z}_2G$; two such submodules are comparable if and only if that is directly visible (using the relations $2^jv_4\mathbb{Z}_2G \geq 2^{j+1}V \leq 2^jv_5\mathbb{Z}_2G$) from the way we have written them.

The diagram $S(V)\backslash\{0\}$ is the following.



6.

Submodule structure of $U \oplus V$

Consider an arbitrary T-submodule M of $U\varepsilon e \oplus V\varepsilon e$. Put

$$M \cap \mathbb{Z}_2 u_i = 2^{u(i)} \mathbb{Z}_2 u_i ,$$

$$M \cap \mathbb{Z}_2 v_j = 2^{v(j)} \mathbb{Z}_2 v_j$$

(using the convention $2^{\infty} = 0$ when some of these intersections are 0), and

$$N = \left(\bigoplus_{i=1}^{5} 2^{u(i)} \mathbb{Z}_2 u_i \right) \oplus \left(\bigoplus_{j=4}^{5} 2^{v(j)} \mathbb{Z}_2 v_j \right) .$$

As the $4e_5(i, i)$ and the $4e_2(j, j)$ are in T , we can conclude that

$$4M \leq N .$$

Since $M \cap U\varepsilon e$ is a T-submodule and the $e_5(i, i)$ are all in T_U , we have $M \cap U\varepsilon e = \oplus \left(M \cap U\varepsilon e \cap \mathbb{Z}_2 u_i \right) = \oplus \left(M \cap \mathbb{Z}_2 u_i \right)$, and a similar statement for $M \cap V\varepsilon e$. Therefore

$$N = (M \cap U\varepsilon e) \oplus (M \cap V\varepsilon e) ,$$

the $u(i)$ *satisfy* 5.1,

and

the $v(j)$ *satisfy* 5.3.

In particular if one of the $v(j)$ is ∞ , so is the other, and then $M \cap V\varepsilon e = 0$; thus $4M \leq N = M \cap U\varepsilon e$ and hence $M \leq U\varepsilon e$. This case has been covered fully in the previous section, as has the case $M \leq V\varepsilon e$. For

the submodules M which require further investigation, we therefore have that

all the $u(i)$ *and* $v(j)$ *are nonnegative integers.*

Next we exploit that T contains $e_5(i, i)$ when $i \leq 3$ and $e_5(j, j) \oplus e_2(j, j)$ when $j > 3$, to conclude that

$$M = \left(\bigoplus_{i=1}^{3} [M \cap \mathbb{Z}_2 u_i] \right) \oplus \left(\bigoplus_{j=4}^{5} [M \cap (\mathbb{Z}_2 u_j \oplus \mathbb{Z}_2 v_j)] \right) .$$

The first three summands are, of course, just the $2^{u(i)}\mathbb{Z}_2 u_i$; the last two need to be looked at more closely.

Take the case $j = 5$ first. We have

$$(M \cap (\mathbb{Z}_2 u_5 \oplus \mathbb{Z}_2 v_5)) \Big/ \left(2^{u(5)}\mathbb{Z}_2 u_5 \oplus 2^{v(5)}\mathbb{Z}_2 v_5 \right)$$
$$\leq (\mathbb{Z}_2 u_5) \Big/ \left(2^{u(5)}\mathbb{Z}_2 u_5 \right) \oplus (\mathbb{Z}_2 v_5) \Big/ \left(2^{v(5)}\mathbb{Z}_2 u_5 \right) .$$

Here the right hand side is a direct sum of two cyclic 2-groups, and the left hand side is a subgroup which avoids both direct summands. Moreover, $2e_5(5, 5) \in T$ implies that this subgroup has exponent at most 2. Forgetting our complex context for a moment, it is a trivial exercise that in such a direct sum there is only one such subgroup apart from 0. (Of course, if one or both cyclic direct summands degenerate, there is no non-zero subgroup of this kind.) We shall find it convenient to state the conclusion in the following form: $M \cap (\mathbb{Z}_2 u_5 \oplus \mathbb{Z}_2 v_5)$ is generated (as additive group) by $2^{u(5)}\mathbb{Z}_2 u_5 \oplus 2^{v(5)}\mathbb{Z}_2 v_5$ and $n\left(2^{u(5)-1}u_5 + 2^{v(5)-1}v_5\right)$ where n is 0 or 1, and if $n = 1$ then $u(5) \geq 1$ and $v(5) \geq 1$.

Similar considerations apply to the case $j = 4$. Again, we have to identify subgroups avoiding both summands in a direct sum of two cyclic 2-groups, but now we can only say that the subgroups of interest have exponent dividing 4 , so we find three nonzero possibilities (fewer when one or both summands have order less than 4). We consolidate the conclusions as follows.

6.1 **LEMMA.** *If M is a T-submodule of $U\varepsilon\varepsilon \oplus V\varepsilon\varepsilon$, then as $\mathbb{Z}_2$-module M is generated by elements*

$$2^{u(i)}u_i \ , \qquad 1 \le i \le 5 \ ,$$

$$2^{v(j)}v_j \ , \qquad 4 \le j \le 5 \ ,$$

$$k\left(2^{u(4)-1}u_4+2^{v(4)-1}v_4\right) \ ,$$

$$l\left(2^{u(4)-2}u_4+2^{v(4)-2}v_4\right) \ ,$$

$$m\left(2^{u(4)-2}u_4-2^{v(4)-2}v_4\right) \ ,$$

$$n\left(2^{u(5)-1}u_5+2^{v(5)-1}v_5\right) \ ,$$

where

(1) *the $u(i)$ and $v(j)$ are nonnegative integers or ∞ , subject to* 5.1 *and* 5.3, *and if any ∞ occurs then $k = l = m = n = 0$;*

(2) *$k, l, m, n \in \{0, 1\}$ and $k + l + m \le 1$;*

(3) *if $k = 1$ then $u(4) \ge 1$ and $v(4) \ge 1$,*
if $l + m = 1$ then $u(4) \ge 2$ and $v(4) \ge 2$,
if $n = 1$ then $u(5) \ge 1$ and $v(5) \ge 1$. //

We now consider any $\mathbb{Z}_2$-submodule M of $U\varepsilon\varepsilon \oplus V\varepsilon\varepsilon$ generated by the elements listed in 6.1 with the parameters satisfying the conditions of 6.1.

For any element of $U\varepsilon e \oplus V\varepsilon e$ expressed in terms of the basis $u_1, \ldots, v_5$, it is straightforward to decide whether it lies in M. Thus we are well prepared to find a necessary and sufficient set of conditions (in terms of the parameters $u(1), \ldots, n$ of M) for M to admit T. Indeed, the conditions already imposed on the parameters clearly ensure that M admits the following subset of T:

$$\left\{2^{a(i,j)}e_5(i, j) \mid 1 \leq i \leq 3\right\} \cup \{e_5(j, j) \oplus e_2(j, j) \mid 4 \leq j \leq 5\} .$$

In the course of the proof of 4.11, we saw that the union of this subset with

$$\left\{2^{a(i,j)}e_5(i, j) \mid i > 3 \geq j\right\}$$

$$\cup \{2e_5(4, 5) \oplus 2e_2(4, 5), 2e_5(5, 4) \oplus 2e_2(5, 4)\}$$

generates T. Thus we need only write down the conditions which express that M contains the image of each of its given generators by each of the (eight) elements of the last displayed subset. The list of simple conditions so obtained is long and highly redundant; we shall not write it out here. Instead, we include a shorter but trivially equivalent list in the following statement, which also takes advantage of the connection established, via 2.1 and 2.2, between T-submodules of $U\varepsilon e \oplus V\varepsilon e$ and $\mathbb{Z}_2G$-submodules of $U \oplus V$.

6.2 THEOREM. *The $\mathbb{Z}_2G$-submodules of $U \oplus V$ are in one-to-one correspondence with the ordered* 11*-tuples*

$$(u(1), \ldots, u(5), v(4), v(5); k, l, m, n)$$

which satisfy conditions (1), (2), (3) *of* 6.1 *and also the following:*

(4) *If* $k = 1$ *then* $u(4) + 1 \geq \max\{u(1), u(2), u(3)\}$ *and*

either $u(4) \geq u(5)$ *and* $v(4) \geq v(5)$

or $u(4) = u(5) - 1$ *and* $v(4) = v(5) - 1$ *and* $n = 1$.

(5) *If* $l + m = 1$ *then* $u(4) \geq \max\{u(1), u(2), u(3)\}$ *and*

either $u(4) = u(5) + 1$ *and* $v(4) = v(5) + 1$

or $u(4) = u(5)$ *and* $v(4) = v(5)$ *and* $n = 1$.

(6) *If* $n = 1$ *then* $u(5) \geq \max\{u(1)-1, u(2), u(3)\}$ *and*

either $u(4) \leq u(5)$ *and* $v(4) \leq v(5)$

or $u(4) = u(5) + 1$ *and* $v(4) = v(5) + 1$ *and* $k + l + m = 1$.

The submodule corresponding to these parameters is generated, as $\mathbb{Z}_2G$-*module, by the elements listed in* 6.1. *It contains the submodule corresponding to* $(u'(1), \ldots, n')$ *if and only if the following conditions hold.*

(7) $u(i) \leq u'(i)$ *for* $1 \leq i \leq 5$, $v(j) \leq v'(j)$ *for* $4 \leq j \leq 5$.

(8) *If* $k' = 1$ *then*

either $u(4) \leq u'(4) - 1$ *and* $v(4) \leq v'(4) - 1$

or $u(4) = u'(4)$ *and* $v(4) = v'(4)$ *and* $k + l + m = 1$ . .

(9) *If* $l' + m' = 1$ *then*

either $u(4) \leq u'(4) - 2$ *and* $v(4) \leq v'(4) - 2$

or $u(4) = u'(4) - 1$ *and* $v(4) = v'(4) - 1$ *and* $k + l + m = 1$

or $u(4) = u'(4)$ *and* $v(4) = v'(4)$ *and* $l = l'$ *and* $m = m'$.

(10) *If* $n' = 1$ *then*

either $u(5) \leq u'(5) - 1$ *and* $v(5) \leq v'(5) - 1$

or $u(5) = u'(5)$ *and* $v(5) = v'(5)$ *and* $n = 1$.

The conditions (7)-(10) are also obtained in the context of 6.1 and $U\varepsilon e \oplus V\varepsilon e$; their derivation is merely tedious, and is omitted. The submodule lattice $S(U \oplus V)$ is clearly much more complicated than $S(U)$ or $S(V)$: it contains the direct product of these two lattices (as the sublattice consisting of the submodules with $k = l = m = n = 0$) but it is not distributive and this makes it hard to visualize; we present no diagrams. The parameters of the sum and intersection of two submodules may be calculated from the parameters of the components, but the best algorithms we could find for these calculations are rather complicated. They are special cases of the algorithms given in the Appendix.

7.

SUBMODULE STRUCTURE OF W

In this section we conclude the study of our "Lie modules" by determining all $\mathbb{Z}_2G$-submodules of W. The key step is the following.

7.1 **LEMMA.** *The $\mathbb{Z}_2G$-submodule of $U \oplus V$ generated by $u_4 - v_4$ is $4W$. In the sense of* 6.2, *the parameters of this submodule are* $(2, 2, 2, 2, 2, 2, 2; 0, 0, 1, 1)$.

Proof. These parameter values satisfy the conditions of 6.2, and the corresponding submodule obviously contains $u_4 - v_4$. Conversely, 4.11 may be used to deduce that each generator of this submodule given by 6.2 is contained even in $(u_4 - v_4)T$.

The claim that this submodule is $4W$ hinges on the fact that W is generated as $\mathbb{Z}_2G$-module by $tzxy$. We show that $4tzxy$ is contained in our submodule: that will be sufficient, for

$$u_4 - v_4 = c_7 - d_7 = a_7 - b_7 = 4yxxz - 4(yx)(xz) \in 4W .$$

The parameters of our submodule show that it contains $4v_4$, $4v_5$, and $2u_5 + 2v_5$. In particular, it contains $4V$ (the $\mathbb{Z}_2G$-submodule generated by $4v_4$ and $4v_5$). It follows also that it contains $2u_5 - 2v_5$ $(= 2u_5 + 2v_5 - 4v_5)$ and $u_4 + 3v_4$ $(= u_4 - v_4 + 4v_4)$. Translating back through the various changes of bases, the first of these may be evaluated as

$$2u_5 - 2v_5 = 2(c_{12}-d_{12}) = 2(a_{10}+a_{11}+a_{12}-b_{10}-b_{11}-b_{12})$$

$$=-4txyz - 4tyzx - 4tzxy \ .$$

Similarly,

$$(u_4+3v_4)(3 \to 4) = (c_7+3d_7)(3 \to 4) = c_{10} + c_{11} + 3d_{10} + 3d_{11}$$

$$= a_{10} + a_{11} - 2a_{12} - 3b_{10} + 3b_{11}$$

$$= 4txyz + 4tyzx - 8tzxy - 8(tx)(yz) + 4(ty)(zx) + 4(tz)(xy) \ .$$

The last three summands here lie in $4V$ and hence in our submodule, so $4txyz + 4tyzx - 8tzxy$ is in our submodule. Adding to it the element previously evaluated, we find that $-12tzxy \in (u_4-v_4)\mathbb{Z}_2G$. As -3 is a unit in $\mathbb{Z}_2$, this completes the proof.

(This argument is related to 34.45 of Hanna Neumann's book [14].)

Now a direct application of 6.2 yields a variant of 6.2 for all submodules of $4W$. As $W \to 4W$, $w \mapsto 4w$ is an isomorphism, that result may be translated into the following description of all submodules of W .

7.2 **THEOREM.** *The $\mathbb{Z}_2G$-submodules of W are in one-to-one correspondence with the ordered 11-tuples*

$$(u(1), \ldots, u(5), v(4), v(5); k, l, m, n)$$

which satisfy the conditions (1), (2) *of* 6.1, *the conditions* (4), (5), (6) *of* 6.2, *and the following conditions.*

(11) *If* $k = 1$ *then*

$$\text{either } u(4) \geq 1 \text{ and } v(4) \geq 1$$

$$\text{or } u(4) = v(4) \ .$$

(12) *If* $l = 1$ *then*

either $u(4) \geq 2$ *and* $v(4) \geq 2$

or $u(4) = v(4) = 1$.

(13) *If* $m = 1$ *then*

either $u(4) \geq 2$ *and* $v(4) \geq 2$

or $u(4) = v(4)$.

(14) *If* $n = 1$ *then*

either $u(5) \geq 1$ *and* $v(5) \geq 1$

or $u(5) = v(5)$.

The submodule corresponding to these parameters is generated, as $\mathbb{Z}_2G$-*module, by the elements listed in* 6.1. *It contains the submodule corresponding to the parameters* $(u'(1), \ldots, n')$ *if and only if conditions* (7), (8), (9), (10) *of* 6.2 *are satisfied.*

Note that the conditions (11), (12), (13), (14), which replaced (3) of 6.1, allow four problematic expressions to occur in the lists of generators of submodules: namely $2^{-1}u_4 \pm 2^{-1}v_4$, $2^{-2}u_4 - 2^{-2}v_4$, and $2^{-1}u_5 + 2^{-1}v_5$. These should be handled with some care, as for instance $2^{-2}u_4$ has no separate reality in W . Nevertheless, as we have seen in the proof of 7.1, there is an element [namely $yxxz - (yx)(xz)$] in W which can be thought of as $2^{-2}u_4 - 2^{-2}v_4$, and of course that is the intended interpretation of this formal expression. The other three problem cases are resolved similarly. This minor inconvenience seems preferable to making the formalism of 7.2 still more complicated.

The lattice $S(W)$ of submodules of W is too complicated to visualize. The algorithms in the Appendix can be used to calculate the parameters of sums and intersections of submodules from the parameters of those submodules.

It is a corollary of 7.2 that U and V are the only isolated proper, nonzero $\mathbb{Z}_2G$-submodules of W. Their parameters are:

$$U = (0, 0, 0, 0, 0, \infty, \infty; 0, 0, 0, 0) ,$$
$$V = (\infty, \infty, \infty, \infty, \infty, 0, 0; 0, 0, 0, 0) ,$$

while in line with 7.1 we have

$$W = (0, \ldots, 0, 1, 1) .$$

Of course,

$$0 = (\infty, \ldots, \infty; 0, 0, 0, 0) .$$

It is straightforward to recognize from the parameters, just by the occurrences of ∞, what the isolator of any particular $\mathbb{Z}_2G$-submodule is. Also, the exponent of the quotient of the isolator modulo the submodule may be readily determined: for example, if the submodule has parameters $(u(1), \ldots, n)$ with no ∞ among them, then the exponent of the quotient of W over this submodule is the maximum of the following list of numbers:

$2^{u(1)}$, $2^{u(2)}$, $2^{u(3)}$;

$2^{u(4)+2}$ and $2^{v(4)+2}$ unless $u(4) = v(4)$ and $k + l + m = 1$

in which case these two numbers are replaced by $2^{u(4)+k+l}$;

$2^{u(5)+1}$ and $2^{v(5)+1}$ unless $u(5) = v(5)$ and $n = 1$ in which case these two numbers are replaced by $2^{u(5)}$.

These examples illustrate the kind of information one can derive from 7.2. It is also true that the long argument which culminated in 7.2 implicitly enables one to decide, for any element of W and for any submodule given by its parameters, whether the element lies in the submodule. To make this claim formal and to elaborate a general algorithm is beyond the scope of this thesis.

8.

THE LAST TERM OF F

At last we are ready to turn to the project outlined in the Introduction. Let F be the free nilpotent group of class 4 freely generated by x, y, z, t : our task is to determine the $2'$-isolated fully invariant subgroups of F . Let N_3 denote the last nontrivial term $\underline{\underline{N}}_3(F)$ of the lower central series of F . As we mentioned in the Introduction to our Section 3, the Magnus-Witt argument elaborated in Section 3 of Kovács [9] admits an obvious adaptation which yields that the $2'$-isolated fully invariant subgroups of F contained in N_3 are in one-to-one correspondence with the $\mathbb{Z}_2G$-submodules of the module W we have been studying so far. Moreover, the nature of that correspondence is such that if Lie ring sums are replaced by group products and Lie products by group commutators, most of the detail we have uncovered can be translated from W to N_3 . We have deliberately used x, y, z, t in both contexts. Expressing the $\mathsf{u}_i, \mathsf{v}_j$ of W in terms of x, y, z, t allows one to identify the corresponding elements of N_3 , to which we transfer the names $\mathsf{u}_1, \ldots, \mathsf{v}_5$: from now on,

$$\mathsf{u}_1 = [y, x, x, y][y, x, x, x][x, y, y, y]^{-1} ,$$

$$\mathsf{u}_2 = [y, x, x, y]^2[y, x, x, x] ,$$

$$u_3 = [y, x, x, z]^3[z, x, x, y]^{-1}[y, x,, x, z]^{-3}\cdot$$
$$\cdot[z, y, y, x]^3[x, y, y, z]^{-1}[z, y,, y, x]^{-3}\cdot$$
$$\cdot[x, z, z, y]^3[y, z, z, x]^{-1}[x, z,, z, y]^{-3} ,$$

$$u_4 = [y, x, x, z]^4[y, x,, x, z]^{-3} ,$$

$$u_5 = [t, x, y, z]^{-2}[t, y, z, x]^{-2}[t, z, x, y]^{-2}\cdot$$
$$\cdot[t, x,, y, z]\ [t, y,, z, x]\ [t, z,, x, y] ,$$

$$v_4 = [y, x,, x, z] ,$$

$$v_5 = [t, x,, y, z][t, y,, z, x][t, z,, x, y] .$$

(Commutators without double commas are to be read as left-normed, so $[y, x, x, y] = [[[y, x], x], y]$, while $[y, x,, x, z]$ stands for $[[y, x], [x, z]]$, and so on.) The translation of 7.2 is the following.

8.1 THEOREM. *The 2'-isolated fully invariant subgroups of F contained in $\underline{\underline{N}}_3(F)$ are in one-to-one correspondence with the ordered 11-tuples*

$$(u(1), \ldots, u(5), v(4), v(5); k, l, m, n)$$

which satisfy conditions (1), (2) *of* 6.1, (4), (5), (6) *of* 6.2, *and* (11), (12), (13), (14) *of* 7.2. *The subgroup corresponding to these parameters is generated (as fully invariant subgroup of F) by the following elements:*

$$u_i^{2^{u(i)}} \quad \textit{with} \quad 1 \le i \le 5$$
$$v_j^{2^{v(j)}} \quad \textit{with} \quad 4 \le j \le 5 ,$$

$$\left(u_4^{2^{u(4)-1}} v_4^{2^{v(4)-1}}\right)^k ,$$

$$\left(u_4^{2^{u(4)-2}} v_4^{2^{v(4)-2}}\right)^l ,$$

$$\left(u_4^{2^{u(4)-2}} v_4^{-2^{v(4)-2}}\right)^m ,$$

$$\left(u_5^{2^{u(5)-1}} v_5^{2^{v(5)-1}}\right)^n ,$$

$$[y, x, x, y]^{2^u} \qquad \textit{where} \quad u = \max\{u(1), \ldots, u(5)\} ,$$

$$[t, x,, y, z]^{2^v} \qquad \textit{where} \quad v = \max\{v(4), v(5)\} .$$

It contains the fully invariant subgroup corresponding to the parameters $(u'(1), \ldots, n')$ *if and only if conditions* (7), (8), (9), (10) *of* 6.2 *are satisfied.*

The convention $2^\infty = 0$ remains in force. The explanatory paragraph after 7.2 translates as follows:

$$u_4^{2^{-1}} v_4^{2^{-1}} = [y, x, x, z]^2 [y, x,, x, z]^{-1} ,$$

$$u_4^{2^{-1}} v_4^{-2^{-1}} = [y, x, x, z]^2 [y, x,, x, z]^{-2} ,$$

$$u_4^{2^{-2}} v_4^{-2^{-2}} = [y, x, x, z][y, x,, x, z]^{-1} ,$$

$$u_5^{2^{-1}} v_5^{2^{-1}} = [t, x, y, z]^{-1} [t, y, z, x]^{-1} [y, z, x, y]^{-1} \cdot$$
$$\cdot [t, x,, y, z] \; [t, y,, z, x] \; [t, z,, x, y]$$

give the interpretation of formally nonsensical expressions which sometimes occur in the list of generators in 8.1. The parameters of N_3 are $(0, \ldots, 0, 1, 1)$. The isolated, nontrivial fully invariant subgroups of

F properly contained in N_3 are: the second derived group F'', with parameters $(\infty, \ldots, \infty, 0, 0; 0, \ldots, 0)$; and the verbal subgroup corresponding to the $\underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4$, with parameters $(0, \ldots, 0, \infty, \infty; 0, \ldots, 0)$. The generators $[y, x, x, y]^{2^u}$ and $[t, x,, y, z]^{2^v}$ are included in 8.1 to ensure that the fully invariant subgroup closure of the elements listed is $2'$-isolated, having 2-power index in one or another isolated fully invariant subgroup. (For the justification of the fact that the fully invariant closure of $[y, x, x, y]$ is isolated, see [5], where use is made of our Lemma 3.2 in this context.) It is easy to see that the factor group of the isolator of the subgroup with parameters $(u(1), \ldots, n)$, over that subgroup, has exponent dividing

$$2^u \qquad \text{when} \quad u < \infty = v ,$$

$$2^v \qquad \text{when} \quad u = \infty > v ,$$

$$2^{2+\max\{u,v\}} \qquad \text{when} \quad u < \infty > v .$$

(Of course, that factor group is trivial when $u = v = \infty$.)

9.

THE COMMUTATOR SUBGROUP F'

The aim of this section is to indicate how we determine the 2'-isolated fully invariant subgroups of F which lie in F'. To this end, we need some details from the well-known classification of varieties of nilpotent groups of class at most 3 (see Jonsson [7], Remeslennikov [17]). We write $\underline{\underline{N}}_2(F) = N_2$ and, as before, $\underline{\underline{N}}_3(F) = N_3$.

9.1. The 2'-isolated fully invariant subgroups H_1 of F such that $N_3 < H_1 \leq F'$ but $H_1 \not\leq N_2$, are in one-to-one correspondence with the ordered pairs (r, s) of nonnegative integers such that $r \geq s$; the subgroup corresponding to this pair being $\underline{\underline{B}}_{2^r}(F')N_2^{2^s}N_3$.

9.2. The 2'-isolated fully invariant subgroups H_2 of F such that $N_3 < H_2 \leq N_2$ are in one-to-one correspondence with the nonnegative integers s, the subgroup corresponding to s being $N_2^{2^s}N_3$.

Here we have written $N_2^{2^s}$ for the subgroup $\{w^{2^s} \mid w \in N_2\}$, a convention we shall employ with any *abelian* group in place of N_2. We shall also use frequently, and without any further reference, the result of [5] that products of 2'-isolated fully invariant subgroups of F are 2'-isolated. Simple commutator calculations show that

$[[x, y]^{2^r}, z] = [x, y, z]^{2^r}$ and $[[x, y, z]^{2^s}, t] = [x, y, z, t]^{2^s}$ in F, so we have the following:

9.3 $$\left[\underline{\underline{B}}_{2^r}(F')N_2^{2^s}N_3,\ F\right] = N_2^{2^r}N_3^{2^s} \quad \text{and} \quad \left[N_2^{2^s}N_3,\ F\right] = N_3^{2^s}.$$

We need two more preparatory results.

9.4 LEMMA. *If two endomorphisms of F agree on F/F', they also agree on $\underline{\underline{B}}_{2^r}(F')N_2^{2^s}N_3/N_2^{2^r}N_3^{2^s}$.*

Proof. Let φ, ψ be endomorphisms of F which agree on F/F'. As is well known, φ and ψ then agree on F'/N_2, on N_2/N_3, and on N_3. In particular, if $a \in F'$ then $a\varphi = (a\psi)w$ for some $w \in N_2$. Since N_2 is central in F', it follows that $a^{2^r}\varphi = (a\varphi)^{2^r} = (a\psi)^{2^r}w^{2^r} = (a^{2^r}\psi)w^{2^r}$; thus φ and ψ agree on the element $a^{2^r}N_2^{2^r}N_3^{2^s}$ of our quotient. By a similar argument, they also agree on the elements $b^{2^s}N_2^{2^r}N_3^{2^s}$ with $b \in N_2$ and $cN_2^{2^r}N_3^{2^s}$ with $c \in N_3$. Our quotient is generated by such elements (as group, not only as fully invariant subgroup), so it follows that φ and ψ agree on it.

Similarly,

9.5 if two endomorphisms of F agree on F/F', they also agree on $N_2^{2^r}N_3/N_3^{2^r}$

Suppose now that H is any $2'$-isolated fully invariant subgroup of F contained in F'. If $H \leq N_3$ then the previous section has dealt with H, so suppose also that $H \nleq N_3$. We have to look at two cases separately.

First, we may have $H \leq N_2$. Then by 9.2 there is a unique nonnegative integer s such that $HN_3 = N_2^{2^s} N_3$. All H which correspond to the same s lie between $N_2^{2^s} N_3$ and $N_3^{2^s}$, for $H \geq [H, F] = [HN_3, F] = N_3^{2^s}$ because N_3 is central in F and 9.3 applies. Thus the study of these H is equivalent to the investigation of the 2'-isolated (End F)-submodules of $N_2^{2^s} N_3 / N_3^{2^s}$. We know from 9.5 that this (2'-torsionfree, central) section of F may as well be viewed as an (End F/F')-module, that is, as $\mathrm{Mat}^{\times}(4, \mathbb{Z})$-module. Hence our earlier methods can handle the problem.

Second, suppose $H \not\leq N_2$. A similar argument using 9.1, 9.3, and 9.4 shows that the study of these subgroups H is equivalent to the investigation of the 2'-isolated submodules of the (2'-torsionfree, central) sections $\underline{\underline{B}}_{2^r}(F') N_2^{2^s} N_3 / N_2^{2^r} N_3^{2^s}$ of F regarded as $\mathrm{Mat}^{\times}(4, \mathbb{Z})$-modules. Thus our previous methods can cope also with this case.

To avoid repetitions, we do not state the outcome of the application of those methods here; it will form part of the statement in the next section.

10.

THE FINAL RESULT

Different methods are needed to cope with the 2′-isolated subgroups H of F which are not contained in F'. The starting point here is that each such H must be of the form $(F' \cap H)\underline{\underline{B}}_{2^q}(F)$ for some nonnegative integer q, which is identified by taking 2^q to be the exponent of F/H. This is virtually a paraphrase of B.H. Neumann's classic result (12.12 in Hanna Neumann's book [14]) that each law is equivalent to an exponent law and a commutator law. Of course, $F' \cap H \geq F' \cap \underline{\underline{B}}_{2^q}(F)$; conversely, if H_1 is any 2′-isolated fully invariant subgroup of F between $F' \cap \underline{\underline{B}}_{2^q}(F)$ and F', then for H defined by $H = H_1\underline{\underline{B}}_{2^q}(F)$ one has that the exponent of F/H is 2^q and $F' \cap H = H_1$. Thus the general problem is reduced to identifying the $F' \cap \underline{\underline{B}}_{2^q}(F)$ in terms of the (yet to be stated) parametrization of the 2′-isolated fully invariant subgroups of F in F'. In those terms, one can then recognize the H_1 which lie between $F' \cap \underline{\underline{B}}_{2^q}(F)$ and F'. (In fact, we shall subsume that parametrization in a more general result.)

We can ignore the cases $q = 0$ and $q = 1$, for then $\underline{\underline{B}}_{2^q}(F) \geq F'$; so henceforth $q \geq 2$. Our aim here is to prove that $F' \cap \underline{\underline{B}}_{2^q}(F)$ is the fully invariant closure of $[y, x]^{2^{q-1}} u_1^{2^{q-2}}$ and $\underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$. This is good enough to enable one to complete the work; the subsequent details

follow the pattern we have already established, and instead of elaborating them we proceed direct to the statement of the main result.

For simplicity, write $F' \cap \underline{\underline{B}}_{2^q}(F)$ as D .

The first step is to quote again from the classification of varieties of nilpotent groups of class at most 3 :

10.1 $$DN_3 = \underline{\underline{B}}_{2^{q-1}}(F')N_2^{2^{q-1}}N_3 .$$

(Strictly speaking, the left hand side has to be rewritten as $F' \cap \underline{\underline{B}}_{2^q}(F)N_3$, using the modular law, before we are entitled to quote.)

By 9.3, $D \geq N_2^{2^{q-1}}$; as obviously $D \geq \underline{\underline{B}}_{2^q}(F')$, we already have that

10.2 $$D \geq \underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}} .$$

We shall use repeatedly the following fact.

10.3 **LEMMA.** *If u, v are elements of a nilpotent group C of class at most 3 , then $u^{2^q}v^{2^q} \equiv (uv)^{2^q}$ modulo $(C')^{2^{q-1}}$.*

The proof is a straightforward collection, a special case of Lemma 10.6 below, so we omit it. For the first application, we take C as the subgroup of F generated by x and $[x, y]$ and note that now $C' \leq N_2$, so we may conclude that

$$[x^{2^q}, y] = x^{-2^q}(x[x, y])^{2^q} \equiv [x, y]^{2^q} \text{ modulo } N_2^{2^{q-1}} ,$$

and hence $[x^{2^q}, y] \in \underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$. This observation shows that

10.4 $\underline{\underline{B}}_{2^q}(F)/\underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$ is a central section of F .

For the second application of 10.3, let a be any element of F and φ, ψ two endomorphisms of F which agree on F/F' , so $a\varphi = (a\psi)b$ for some element b of F' . Take C as the subgroup generated by $a\psi$ and b , noting that again $C' \leq N_2$. Now 10.3 yields that

$$a^{2^q}\varphi = (a\varphi)^{2^q} = \big((a\psi)b\big)^{2^q} \equiv \big(a^{2^q}\psi\big)b^{2^q} \quad \text{modulo} \quad N_2^{2^{q-1}} ,$$

so φ and ψ agree on the element $a^{2^q}\underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$ of the section considered in 10.4. That section is generated by such elements (as group, not only as fully invariant subgroup), so we may conclude that

10.5 if two endomorphisms of F agree on F/F' , they also agree on $\underline{\underline{B}}_{2^q}(F)/\underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$.

Let d be the element of D defined by

$$(xy)^{2^q} = x^{2^q}y^{2^q}d ,$$

and let D_1 be the fully invariant closure of d and $\underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}}$ in F . The next step is to prove that $D_1 = D$. Clearly, $D \geq D_1$. We know that $\underline{\underline{B}}_{2^q}(F)/D \cong \underline{\underline{B}}_{2^q}(F)F'/F' = \underline{\underline{B}}_{2^q}(F/F')$, so $\underline{\underline{B}}_{2^q}(F)/D$ is free abelian of

rank 4 , and therefore it cannot be written as a *proper* homomorphic image of any 4-generator abelian group. Thus $D = D_1$ will follow if we can establish that $\underline{\underline{B}}_{2^q}(F)/D_1$ is a 4-generator abelian group. We already know, from 10.4, that it is abelian; we shall now show that it is generated by $x^{2^q}D_1, \ldots, t^{2^q}D_1$. To this end, it is clearly sufficient to show that the subgroup of $\underline{\underline{B}}_{2^q}(F)/D_1$ generated by these elements admits all endomorphisms of F . This subgroup obviously admits all endomorphisms which merely permute or power the generators x, y, z, t . It also admits the endomorphism which maps x to xy and leaves y, z, t fixed: for, this will map $x^{2^q}D_1$ to $(xy)^{2^q}D_1$ which is equal to $\left(x^{2^q}D_1\right)\left(y^{2^q}D_1\right)$ by the definition of D_1 . We know from 2.7 that each endomorphism of F will agree on F/F' with some composite of the endomorphisms just considered; hence it follows by 10.5 that our subgroup will admit it. This establishes that $D_1 = D$.

To reach our stated aim, it remains to prove that

$$d \equiv [x, y]^{2^{q-1}} u_1^{2^{q-2}} \quad \text{modulo} \quad \underline{\underline{B}}_{2^q}(F')N_2^{2^{q-1}} .$$

At this point, one cannot avoid a complicated collection to find out just what d is.

10.6 LEMMA.

$$(xy)^{2^q} = x^{2^q} y^{2^q} [y, x]^{\alpha}[y, x, x]^{\beta}[x, y, y]^{\gamma}[y, x, x, x]^{\delta} u_1^{\varepsilon}$$

where

$$\alpha = \binom{2^q}{2} \equiv 2^{q-1} \pmod{2^q} ,$$

$$\beta = \binom{2^q}{3} \equiv 0 \pmod{2^{q-1}} ,$$

$$\gamma = -\binom{2^q}{3} - \binom{2^q+1}{3} \equiv 0 \pmod{2^{q-1}} ,$$

$$\delta = \quad - 2\binom{2^q+1}{4} \equiv 0 \pmod{2^{q-1}} ,$$

$$\varepsilon = \binom{2^q}{4} + 2\binom{2^q+1}{4} \equiv 2^{q-2} \pmod{2^{q-1}} ,$$

This confirms the claim concerning d ; the straightforward but tedious proof is omitted, as is the remaining detail which leads to our main result.

We recall the convention $2^\infty = 0$, and supplement it by the usual $\infty \pm 1 = \infty$. It will be convenient to have the following shorthand available: $(u'(1), \ldots, v'(5); k', l', m', n') \leq M$ will mean that $u'(1), \ldots, n'$ satisfy the conditions (7), (8), (9), (10) of 6.2; when s is a nonnegative integer, we write $2^s W$ for $(s, \ldots, s; 0, 0, 1, 1)$.

10.7 **THEOREM.** *The 2'-isolated fully invariant subgroups of F are in one-to-one correspondence with the ordered 16-tuples*

$$(q; r; s; u(1), \ldots, u(5), v(4), v(5); i; j; k, l, m, n)$$

which satisfy conditions (1), (2) *of* 6.1, (4), (5), (6) *of* 6.2, (11), (12), (13), (14) *of* 7.2, *and the following.*

(15) *q, r, s are nonnegative integers or ∞, while $i, j \in \{0, 1\}$.*

(16) *If $q \le 1$ then $r = 0$.*

(17) *If $r = 0$ then the 16-tuple is*

$$(q; 0; 0; 0, \ldots, 0; 0; 0; 0, 0, 1, 1) .$$

(18) *If $q \ge 2$ and $r \ge 1$ then $s \le q - 1$, $s \le r$, either $s = \infty$ or $2^s W \le M$, and*

either $r \le q - 1$ and $u(1) \le q - 2$ and $u(4) \le r - 1$
or $r = q$ and $u(1) = q - 1$ and $i = 1$.

(19) *If $i = 1$ then $1 \le u(1) \le s < r < \infty$ and*

$$\big(u(1), u(1), u(1)-1, u(1), u(1)-1, r-1, r-1; 1, 0, 0, 0\big) \le M .$$

(20) *If $j = 1$ then $1 \le u(2) < s < \infty$ and $2^{s-1} W \le M$ and*

$$u(2) \ge \max\{u(1)-1, u(3), u(4), u(5)+1\} .$$

The corresponding subgroup of F is the fully invariant closure of

$$x^{2^q}, [y, x]^{2^r}, [y, x, z]^{2^s},$$

$$\left([y, x]^{2^{r-1}} u_1^{2^{u(1)-1}}\right)^i, \left([y, x, x]^{2^{s-1}} u_2^{2^{u(2)-1}}\right)^j,$$

and the elements listed in 8.4. It contains the subgroup corresponding to $(q'; \ldots, n')$ if and only if $q \le q'$, $r \le r'$, $s \le s'$, $\big(u'(1), \ldots, n'\big) \le M$, and

(21) *if $i' = 1$ then*

either $r \leq r' - 1$ *and* $u(1) \leq u'(1) - 1$

or $r = r'$ *and* $u(1) = u'(1)$ *and* $i = 1$;

(22) *if* $j' = 1$ *then*

either $s \leq s' - 1$ *and* $u(2) \leq u'(2) - 1$

or $s = s'$ *and* $u(2) = u'(2)$ *and* $j = 1$.

It follows, in particular, that the subgroup $\underline{B}_4(F)$ corresponds to

$$(2;\ 2;\ 1;\ 1,\ 1,\ 0,\ 1,\ 0,\ 1,\ 0;\ 1;\ 0;\ 0,\ 0,\ 1,\ 0) .$$

This has been compared and found to agree with the known structure of the Burnside group $B(4, 4)$ (see, for instance, Hall [6]). The isolated fully invariant subgroups are readily identified as those with all parameters in $\{0, \infty\}$ except that when the middle group of seven parameters consists of zeros the last two parameters are ones. There is no problem in identifying the parameters of the isolator from the parameters of a subgroup, or in obtaining at least a crude upper estimate for the exponent of their quotient (if p is the sum of the finite parameters of the subgroup, 2^{2+p} will always do). It is implicit in our arguments that, given any subgroup by its parameters and any element of F, one can decide whether the element belongs to the subgroup, but to make this explicit and elaborate an algorithm is beyond the scope of this work.

Since each variety of nilpotent groups of class at most 4 is defined by its 4-variable laws (see 34.15 and 34.34 in Hanna Neumann's book [14]), the result we have reached is equivalent to determining all 2′-torsionfree varieties of nilpotent groups of class at most 4. In view of [5], this completes the task of finding all varieties of nilpotent groups of class at most 4.

APPENDIX

We present here, without proof, algorithms for calculating the parameters of the intersection and of the product of two 2′-isolated fully invariant subgroups of F, from the parameters of the two subgroups. It will be more convenient here to write the parameters of the subgroups X_α ($\alpha = 1, 2$) as

$$(q_\alpha; r_\alpha; s_\alpha; a_\alpha, \ldots, g_\alpha; i_\alpha; j_\alpha; k_\alpha, l_\alpha, m_\alpha, n_\alpha) .$$

THE INTERSECTION ALGORITHM

Step 1. Set $q = \max\{q_1, q_2\}, \ldots, g = \max\{g_1, g_2\}$.

Step 2. Set $i = 1$ if

(i) either $r \geq r_1 + 1$ and $a \geq a_1 + 1$

or $r = r_1$ and $a = a_1$ and $i_1 = 1$;

and (ii) either $r \geq r_2 + 1$ and $a \geq a_2 + 1$

or $r = r_2$ and $a = a_2$ and $i_2 = 1$.

Otherwise set $i = 0$.

Step 3. Set $j = 1$ if

(i) either $s \geq s_1 + 1$ and $b \geq b_1 + 1$

or $s = s_1$ and $b = b_1$ and $j_1 = 1$;

and (ii) either $s \geq s_2 + 1$ and $b \geq b_2 + 1$

or $s = s_2$ and $b = b_2$ and $j_2 = 1$.

Otherwise set $j = 0$.

Step 4. Set $l = 1$ (respectively $m = 1$) if

(i) either $d \geq d_1 + 2$ and $f \geq f_1 + 2$

or $d = d_1 + 1$ and $f = f_1 + 1$ and $k_1 + l_1 + m_1 = 1$

or $d = d_1$ and $f = f_1$ and $l_1 = 1$ (respectively $m_1 = 1$);

and (ii) either $d \geq d_2 + 2$ and $f \geq f_2 + 2$

or $d = d_2 + 1$ and $f = f_2 + 1$ and $k_2 + l_2 + m_2 = 1$

or $d = d_2$ and $f = f_2$ and $l_2 = 1$ (respectively $m_2 = 1$).

Otherwise set $l = 0$ (respectively $m = 0$).

Step 5. Set $k = 1$ if

(i) $l = m = 0$;

and (ii) either $d \geq d_1 + 1$ and $f \geq f_1 + 1$

or $d = d_1$ and $f = f_1$ and $k_1 + l_1 + m_1 = 1$;

and (ii) either $d \geq d_2 + 1$ and $f \geq f_2 + 1$

or $d = d_2$ and $f = f_2$ and $k_2 + l_2 + m_2 = 1$.

Otherwise set $k = 0$.

Step 6. Set $n = 1$ if

(i) either $e \geq e_1 + 1$ and $g \geq g_1 + 1$

or $e = e_1$ and $g = g_1$ and $n_1 = 1$;

and (ii) either $e \geq e_2 + 1$ and $g \geq g_2 + 1$

or $e = e_2$ and $g = g_2$ and $n_2 = 1$.

Otherwise set $n = 0$.

Step 7. The parameters of $X_1 \cap X_2$ are these $q, r, \ldots, n$.

THE PRODUCT ALGORITHM

Step 1. For $\alpha = 1, 2$ set

$$r'_\alpha = \begin{cases} r_\alpha \\ r_\alpha - 1 \end{cases} \quad \text{and} \quad a'_\alpha = \begin{cases} a_\alpha & \text{if } i_\alpha = 0 , \\ a_\alpha - 1 & \text{if } i_\alpha = 1 ; \end{cases}$$

$$s'_\alpha = \begin{cases} s_\alpha \\ s_\alpha - 1 \end{cases} \quad \text{and} \quad b'_\alpha = \begin{cases} b_\alpha & \text{if } j_\alpha = 0 , \\ b_\alpha - 1 & \text{if } j_\alpha = 1 ; \end{cases}$$

$$d'_\alpha = \begin{cases} d_\alpha \\ d_\alpha - 1 \\ d_\alpha - 2 \end{cases} \quad \text{and} \quad f'_\alpha = \begin{cases} f_\alpha & \text{if } k_\alpha = l_\alpha = m_\alpha = 0 , \\ f_\alpha - 1 & \text{if } k_\alpha = 1 , \\ f_\alpha - 2 & \text{if } l_\alpha = 1 \text{ or } m_\alpha = 1 ; \end{cases}$$

$$e'_\alpha = \begin{cases} e_\alpha \\ e_\alpha - 1 \end{cases} \quad \text{and} \quad g'_\alpha = \begin{cases} g_\alpha & \text{if } n_\alpha = 0 , \\ g_\alpha - 1 & \text{if } n_\alpha = 1 . \end{cases}$$

Step 2. Set $q = \min\{q_1, q_2\}$, $c = \min\{c_1, c_2\}$ and otherwise $r'' = \min\{r'_1, r'_2\}, \ldots, g'' = \min\{g'_1, g'_2\}$.

Step 3. Set $i = 1$ if

(i) either $r'' \leq r'_1 - 1$ and $a'' \leq a'_1 - 1$

or $r'' = r'_1$ and $a'' = a'_1$ and $i_1 = 1$;

(ii) either $r'' \leq r'_2 - 1$ and $a'' \leq a'_2 - 1$

or $r'' = r'_2$ and $a'' = a'_2$ and $i_2 = 1$.

Otherwise set $i = 0$.

Step 4. Set $j = 1$ if

(i) either $s'' \le s_1' - 1$ and $b'' \le b_1' - 1$

or $s'' = s_1'$ and $b'' = b_1'$ and $j_1 = 1$;

(ii) either $s'' \le s_2' - 1$ and $b'' \le b_2' - 1$

or $s'' = s_2'$ and $b'' = b_2'$ and $j_2 = 1$.

Otherwise set $j = 0$.

Step 5. Set $l = 1$ (respectively $m = 1$) if

(i) either $d'' \le d_1' - 2$ and $f'' \le f_1' - 2$

or $d'' = d_1' - 1$ and $f'' = f_1' - 1$ and $k_1 + l_1 + m_1 = 1$,

or $d'' = d_1'$ and $f'' = f_1'$ and $l_1 = 1$ (respectively $m_1 = 1$),

and (ii) either $d'' \le d_2' - 2$ and $f'' \le f_2' - 2$

or $d'' = d_2' - 1$ and $f'' = f_2' - 1$ and $k_2 + l_2 + m_2 = 1$,

or $d'' = d_2'$ and $f'' = f_2'$ and $l_2 = 1$ (respectively $m_2 = 1$).

Otherwise set $l = 0$ (respectively $m = 0$).

Step 6. Set $k = 1$ if

(i) $l = m = 0$,

(ii) either $d'' \le d_1' - 1$ and $f'' \le f_1' - 1$

or $d'' = d_1'$ and $f'' = f_1'$ and $k_1 + l_1 + m_1 = 1$;

and (iii) either $d'' \le d_2' - 1$ and $f'' \le f_2' - 1$

or $d'' = d_2'$ and $f'' = f_2'$ and $k_2 + l_2 + m_2 = 1$.

Otherwise set $k = 0$.

Step 7. Set $n = 1$ if

(i) either $e'' \le e_1' - 1$ and $g'' \le g_1' - 1$

or $e'' = e_1'$ and $g'' = g_1'$ and $n_1 = 1$,

and (ii) either $e'' \le e_2' - 1$ and $g'' \le g_2' - 1$

or $e'' = e_2'$ and $g'' = g_2'$ and $n_2 = 1$.

Otherwise set $n = 0$.

Step 8. Set

$$r = \begin{cases} r'' \\ \\ r''+1 \end{cases} \quad \text{and} \quad a = \begin{cases} a'' & \text{if } i = 0 , \\ \\ a''+1 & \text{if } i = 1 ; \end{cases}$$

$$s = \begin{cases} s'' \\ \\ s''+1 \end{cases} \quad \text{and} \quad b = \begin{cases} b'' & \text{if } j = 0 , \\ \\ b''+1 & \text{if } j = 1 ; \end{cases}$$

$$d = \begin{cases} d'' \\ \\ d''+1 \\ \\ d''+2 \end{cases} \quad \text{and} \quad f = \begin{cases} f'' & \text{if } k = l = m = 0 , \\ \\ f''+1 & \text{if } k = 1 , \\ \\ f''+2 & \text{if } l = 1 \text{ or } m = 1 , \end{cases}$$

$$e = \begin{cases} e'' \\ \\ e''+1 \end{cases} \quad \text{and} \quad g = \begin{cases} g'' & \text{if } n = 0 , \\ \\ g''+1 & \text{if } n = 1 . \end{cases}$$

Step 9. The parameters of $X_1 X_2$ are these $q, r, \ldots, n$.

BIBLIOGRAPHY

[1] F.W. Anderson and K.R. Fuller, *Rings and Categories of Modules* (Graduate Texts in Mathematics, 13. Springer-Verlag, New York, Heidelberg, Berlin, 1973).

[2] H. Boerner, *Representations of Groups* (North-Holland, Amsterdam, 1963).

[3] Warren Brisley, "On varieties of metabelian p-groups and their laws", *J. Austral. Math. Soc.* 7 (1967), 64-80.

[4] Warren Brisley, "Varieties of metabelian p-groups of class p, $p + 1$ ", *J. Austral. Math. Soc.* 12 (1971), 53-62.

[5] Patrick Fitzpatrick and L.G. Kovács, "Varieties of nilpotent groups of class four", attached.

[6] M. Hall, Jr., "Notes on groups of exponent four", *Proceedings from a Conference on Group Theory*, Wisconsin, Parkside (Lecture Notes in Mathematics, 319. Springer-Verlag, Berlin, Heidelberg, New York, 1973).

[7] Bjarni Jonsson, "Varieties of groups of nilpotency three", *Notices Amer. Math. Soc.* 13 (1966), 488.

[8] A.A. Kljačko, "Varieties of p-groups of small class" (Russian), *Ordered Sets and Lattices*, No. 1, 31-42 (Izdat. Univ. Saratov, Saratov, 1971).

[9] L.G. Kovács, "Varieties of nilpotent groups of small class", *Topics in Algebra* (Proc. 18th Summer Research Institute, Canberra, 1978, 205-229. Lecture Notes in Mathematics, 697. Springer-Verlag, Berlin, Heidelberg, New York, 1978).

[10] L.G. Kovács, "The thirty-nine varieties", *Math. Scientist* 4 (1979), 113-128.

[11] L.G. Kovács and M.F. Newman, "On non-cross varieties of groups", *J. Austral. Math. Soc.* 12 (1971), 129-144.

[12] W. Magnus, "Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring", *Math. Ann.* **111** (1935), 259-280.

[13] W. Magnus, "Über Beziehungen zwischen höheren Kommutatoren", *J. reine angew. Math.* **177** (1937), 105-115.

[14] Hanna Neumann, *Varieties of Groups* (Ergebnisse der Mathematik und ihrer Grenzgbiete, **37**. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[15] M.F. Newman, "Some varieties of groups", *J. Austral. Math. Soc.* **16** (1973), 481-494.

[16] Paul Pentony, "Laws in torsionfree nilpotent varieties" (PhD thesis, Australian National University, Canberra, 1970).

[17] V.N. Remeslennikov, "Two remarks on 3-step nilpotent groups" (Russian), *Algebra i Logika* **4** (1965), no. 2, 59-66.

[18] G.E. Wall, "Lie methods in group theory", *Topics in Algebra* (Proc. 18th Summer Research Institute, Canberra, 1978, 137-173. Lecture Notes in Mathematics, **697**. Springer-Verlag, Berlin, Heidelberg, New York, 1978).

[19] E. Witt, "Treue Darstellung Liesher Ringe", *J. reine angew Math.* **177** (1937), 152-160.

Varieties of nilpotent groups of class four

Patrick Fitzpatrick and L.G. Kovács

1. Introduction

This is a report on the first and easy half of a project aimed at determining all varieties of nilpotent groups of class (at most) four. The initial step is to reduce the problem to two cases: varieties whose free groups have no nontrivial elements of odd order, dealt with in the first author's thesis [3], and varieties whose free groups have no elements of order 2, determined here. The main result is that the latter varieties form a distributive lattice (with respect to order by inclusion: this is *not* a sublattice of the lattice of all varieties of nilpotent groups of class at most 4) which may be given as follows. Let Ω denote the set consisting of 0 and the odd positive integers partially ordered by divisibility (with the convention that 0 is the *largest* element of Ω). Clearly, Ω is a distributive lattice, with joins and meets being least common multiples and greatest common divisors. Consider the sublattice of the direct product of six copies of Ω which consists of all the (a, b, c, d, e, f) such that

b divides a, c is d or $3d$ and divides b,

d is a common multiple of e and f,

and if 3 divides a then $3d$ also divides a.

This sublattice is isomorphic to the lattice of all varieties of nilpotent groups of class at most 4 whose free groups have no elements of order 2 ; namely, (a, b, c, d, e, f) corresponds to the variety defined by the following laws:

$$x_1^a = [x_1, x_2]^b = [x_1, x_2, x_3]^c = [x_1, x_2, x_1]^d =$$

$$= [x_1, x_2, x_2, x_1]^e = [[x_1, x_2], [x_3, x_4]]^f = [x_1, x_2, x_3, x_4]^{ef} =$$

$$= [x_1, x_2, x_3, x_4, x_5] = 1 .$$

(All incompletely bracketed commutators are to be read as "left-normed": that is, $[x_1, x_2, x_3] = [[x_1, x_2], x_3]$, and so on.)

All varieties of nilpotent groups of class at most 3 were known at least fifteen years ago (Jónsson [9], Remeslennikov [15]). A particularly sharp result of Gupta and Newman [4] on commutator laws led then, among other things, to Brisley's conclusive work [1], [2] on varieties of metabelian p-groups of class at most $p + 1$, from which we derive the metabelian part of our result. On the other hand, varieties of nilpotent p-groups of class at most $p - 1$ have an elaborate theory, with the first significant result of Thrall [16] almost forty years old. The first comprehensive treatment in print is Kljačko's [10]. (He also asserted, without proof, the distributivity of the lattice of all varieties of 3-groups of class at most 4: this is, of course, confirmed by our present results.) Only a small part of this theory is relevant in detail here, although that is used rather heavily: Section 2 of the exposition [11].

There is also a parallel theory for torsionfree varieties of nilpotent groups (that is, varieties whose free groups are torsionfree), developed by Newman and the second author in 1968 but not published until recently [11], [12]. We need the fact, which must have been widely known for quite some time though the only reference seems to be [12], that there are precisely seven torsionfree varieties of nilpotent groups of class at most 4 . Six of them are obvious to pick: in the notation of Hanna Neumann's book [13], they are $\underline{\underline{E}}$, $\underline{\underline{A}}$, $\underline{\underline{N}}_2$, $\underline{\underline{N}}_3$, $\underline{\underline{A}}^2 \cap \underline{\underline{N}}_4$, and $\underline{\underline{N}}_2$ itself. The seventh was called $\underline{\underline{E}}_3$ but left without defining laws in [12]; it was (also) identified there as the variety generated by the torsionfree groups of $\underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4$. Since then, it has come to our attention that the unpublished thesis [14] of Pentony contains a statement (pp 45-46, proof largely suppressed) to the effect that this variety is defined by the laws corresponding to our (0, 0, 0, 0, 1, 0). Let $\underline{\underline{M}}$, say, denote the variety defined by these laws. Clearly, $\underline{\underline{N}}_4 > \underline{\underline{M}} \geq \underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4 \geq \underline{\underline{E}}_3$, so one can indeed conclude that $\underline{\underline{M}} = \underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4 = \underline{\underline{E}}_3$ provided one knows that $\underline{\underline{M}}$ is torsionfree: but it is just this point which Pentony left without any hint of a proof. We show here (as 2.5) that the Gupta-Newman result (loc. cit.) quickly yields that the free groups of $\underline{\underline{M}}$ have no nontrivial elements of odd order; then Lemma 3.2 of [3] gives (via the appropriate version of the Magnus-Witt argument elaborated in Section 3 of [11]) that these groups have no elements of order 2 either. This (confirms Pentony's claim and) establishes that $\underline{\underline{N}}_3^{(2)} \cap \underline{\underline{N}}_4$ is torsionfree and is defined by the laws corresponding to (0, 0, 0, 0, 1, 0): a much more satisfactory identification

of the seventh torsionfree subvariety of $\underline{\underline{N}}_4$ than those given in [12].

We are greatly indebted to Dr M.F. Newman for a continuing exchange of ideas, over many years, on the background to this work.

2. Sylow decomposition

It is well known that each subvariety of $\underline{\underline{N}}_4$ is defined by its 4-variable laws (see 34.15 and 34.34 in [13]), and that therefore our task is equivalent to finding all fully invariant subgroups in the rank 4 free group F of $\underline{\underline{N}}_4$. This is the setting we shall work in throughout the paper.

For each fully invariant subgroup U of F, write

U_0/U for the set of elements of finite order in F/U,

U_2/U for the set of elements of 2-power order in F/U, and

$U_{2'}/U$ for the set of elements of odd order in F/U.

As F/U is finitely generated and nilpotent, U_i/U is a finite subgroup for each i in $\{0, 2, 2'\}$, and U_i is obviously fully invariant in F. It is immediate that

2.1 $U_2 \cap U_{2'} = U$ and $U_2U_{2'} = U_0$,

while

2.2 $(U_i)_i = U_i$ and $(U_i)_j = U_0$ whenever $i \neq j$.

Moreover,

2.3 $(U \cap V)_i = U_i \cap V_i$; in particular, if $U \leq V$ then $U_i \leq V_i$.

Here $(U \cap V)_i \leq U_i \cap V_i$ is obvious; the converse inclusion holds

because $w \in U_i \cap V_i$ means that $w^m \in U$ and $w^n \in V$ for suitable integers m, n, and then $w^{mn} \in U \cap V$. We also need

2.4 $(UV)_i = (U_iV_i)_i$.

Again, $(UV)_i \leq (U_iV_i)_i$ is obvious. To see the converse, note that U_iV_i/UV is a subgroup generated by elements of finite (or 2-power, or odd) orders in the nilpotent group F/UV, and hence consists of such elements.

Now let Λ denote the lattice of all fully invariant subgroups of F, and put $\Lambda_i = \{U \in \Lambda \mid U_i = U\}$. Thus for instance Λ_2 consists of the 2-isolated fully invariant subgroups: that is, of the fully invariant U such that F/U has no elements of order 2. Each Λ_i is partially ordered by inclusion, and is a lattice with respect to this partial order: by 2.2 and 2.3, the meet of U and V in Λ_i is just $U \cap V$, while their join in Λ_i is $(UV)_i$. Thus Λ_i is a sublattice of Λ if and only if $(UV)_i = UV$ for all U, V in Λ_i: we shall see in 2.6 that this is the case when i is $2'$ but not when i is 0 or 2.

Consider the following diagram of maps.

$$\begin{array}{ccccc} & & U & \longmapsto & U_2 \\ U & & \Lambda & \to & \Lambda_2 \quad V \\ \downarrow & & \downarrow & & \downarrow \quad \downarrow \\ U_{2'} & & \Lambda_{2'} & \to & \Lambda_0 \quad V_0 \\ & & W & \longmapsto & W_0 \end{array}$$

By 2.2, the diagram commutes and all four maps are surjective. By

2.3 and 2.4, all the maps are lattice-homomorphisms. (Consequently, the Λ_i are modular, because Λ is.) We therefore also have a lattice-homomorphism of Λ into the direct product lattice $\Lambda_2 \times \Lambda_{2'}$, given by $U \mapsto (U_2, U_{2'})$. The first statement of 2.1 implies that this homomorphism is an embedding. If (V, W) lies in its image then $V_0 = W_0$ by the commutativity of the diagram; conversely, if $(V, W) \in \Lambda_2 \times \Lambda_{2'}$ and $V_0 = W_0$ then 2.2 and 2.3 show that (V, W) is the image of $V \cap W$ and hence lies in the image of Λ. (In technical terms: Λ is the subdirect product of Λ_2 and $\Lambda_{2'}$, defined by the pullback diagram above.) Thus if we know $\Lambda_2 \to \Lambda_0$ and $\Lambda_{2'} \to \Lambda_0$, we can reconstruct Λ. In this sense, the study of all fully invariant subgroups is reduced to the separate studies of the 2-isolated fully invariant subgroups and the 2'-isolated fully invariant subgroups.

The role a fully invariant subgroup U plays in the lattice Λ is not the only thing, perhaps not even the most important thing, we want to know about it. We are certainly interested, for instance, in finding a finite defining set for U (that is, a finite subset of which it is the fully invariant subgroup closure), for such a set (with the class 4 law adjoined) will give a finite basis for the laws of the corresponding variety. Our reduction gives U in terms of U_2 and $U_{2'}$, as $U_2 \cap U_{2'}$; and, in general, there is no known procedure for obtaining a defining set for the intersection $V \cap W$ of two fully invariant subgroups from defining sets of V and W. So it is relevant to observe that there *is* such a procedure when $(V, W) \in \Lambda_2 \times \Lambda_{2'}$, $V_0 = W_0$, provided we have upper estimates

for the (odd) exponent of V_0/V and the (2-power) exponent of W_0/W. Namely, suppose that the subsets R and S define V and W, respectively, and that $V_0/V \in \underline{\underline{B}}_n$ (with n odd) and $W_0/W \in \underline{\underline{B}}_{2^k}$. Let U be the fully invariant subgroup closure of the set T defined by

$$T = \{r^{2^k} \mid r \in R\} \cup \{s^n \mid s \in S\} .$$

As $V_{2'} = (V_2)_{2'} = V_0 = W_0 = (W_{2'})_2 = W_2$ (by 2.2 and the assumptions on V, W), the indices of V and W in this subgroup are coprime, so $VW = V_0 = W_0$. It follows that $V_0/V \cap W = (V/V \cap W) \times (W/V \cap W)$ and $V/V \cap W \cong W_0/W \in \underline{\underline{B}}_{2^k}$, $W/V \cap W \cong V_0/V \in \underline{\underline{B}}_n$. Hence $T \subseteq V \cap W$, so $U \leq V \cap W$. On the other hand, the elements of R have 2-power orders modulo U, so V/U is generated by (endomorphic images of) elements of 2-power order in the finitely generated nilpotent group F/U, and therefore V/U has 2-power order. Similarly, W/U has odd order. Thus $(V/U) \cap (W/U) = 1$, that is, $V \cap W = U$. This proves that T defines $V \cap W$. Note that if R and S are finite, so is T.

Our aim in the rest of the paper is therefore to determine the lattice Λ_2 of all 2-isolated fully invariant subgroups V of F; to identify, for each V, its "isolator" V_0; to give a finite defining set for each V and an upper estimate for the exponent of V_0/V.

Before we embark on this task, there are two other points to settle: the claim made in the introduction concerning Λ_0, and the assertion earlier in this section that of the Λ_i only $\Lambda_{2'}$ is a

sublattice of Λ . Six members of Λ_0 are well known: F itself; the commutator subgroup F' ; the other nontrivial terms of the lower central series, namely $\underline{\underline{N}}_2(F)$ which we rarely have to refer to, and $\underline{\underline{N}}_3(F)$ which we need frequently and denote by N to save writing too much; the second commutator subgroup F" ; and the trivial subgroup 1 . Let $\{x, y, z, t\}$ be a free generating set of F , and M the fully invariant subgroup defined by the (left-normed) commutator $[y, x, x, y]$; we know from [12] that M_0 is the seventh and last member of Λ_0 , with $M_0 < N$ and $M_0 \cap F'' = 1$. A result of Gupta and Newman [4] may be applied to F/MF" , and yields that N/MF" has exponent dividing 4 : that is, $N^4 \leq MF''$ (where N^4 is the subgroup of the abelian group N consisting of the fourth powers of the elements of N). Thus $M_0^4 \leq MF'' \cap M_0 = M(F'' \cap M_0) = M$ (where we have used the modularity of Λ). It follows that $M_{2'} = M$. By Lemma 3.2 of [3], read via an obvious adaption of Section 3 of [11], we have that $M_{2'}$ is isolated: thus

$$M = M_2 = M_{2'} = M_0 .$$

This settles the first point.

From this discussion, we also need $(MF'')_0 = (MF'')_2 = N$ and $(MF'')_{2'} = MF''$ towards the second point. As further preparation, we establish that $MF'' \neq N$. The (standard) wreath product of a group of order 2 by an elementary abelian group of order 8 is a well-known example: a 4-generator metabelian group which is nilpotent of class precisely 4, in which all 2-generator subgroups have class at most 3 (compare 34.54 of [13]). Thus F does have

homomorphisms onto this group, and the kernel of such a homomorphism must contain MF'' but cannot contain N. We are now ready to prove the following.

2.6 For $U, V \in \Lambda_i$ we have $(UV)_i \neq UV$ if and only if $i \neq 2'$ and either $U_0 = M$, $V_0 = F''$ or $U_0 = F''$, $V_0 = M$.

Suppose first that U_0 and V_0 satisfy one of the alternative conditions: then $UV \leq U_0V_0 = MF''$. By 2.4, we have $(UV)_0 = (U_0V_0) = N$. As the nontrivial 2-group N/MF'' is a factor group of $(UV)_0/UV$, neither $(UV)_0/UV$ nor $(UV)_2/UV$ can be trivial. On the other hand, if also $U, V \in \Lambda_{2'}$, then by 2.2 we have $U_0 = U_2$, $V_0 = V_2$, so 2.4 yields $(UV)_2 = (U_2V_2)_2 = (U_0V_0)_2 = (MF'')_2 = N = (UV)_0$; thus $(UV)_0/UV$ is a 2-group and $(UV)_{2'} = UV$. If U_0 and V_0 do not satisfy either condition, then they are comparable: for, on inspecting the seven elements of Λ_0 one finds that M, F'' is the only incomparable pair. Say, $U_0 \leq V_0$. Then $(UV)_0 = (U_0V_0)_0 = V_0$ by 2.4 and 2.2; thus $(UV)_0/UV$ is a factor group of V_0/V. Now $V \in \Lambda_i$ gives that $(UV)_0/UV$ is trivial or a 2'-group or a 2-group, according as i is 0 or 2 or $2'$, so that also $UV \in \Lambda_i$, that is, $(UV)_i = UV$. This completes the proof of 2.6.

A moment's reflection shows that this, with $(MF'')_0 = N = (MF'')_2$, settles everything: $\Lambda_{2'}$ is, but Λ_2 is not, a sublattice of Λ; while Λ_0 is a sublattice of Λ_2, but not of Λ, nor of $\Lambda_{2'}$.

3. Distributivity

The aim of this section is to prove that Λ_2 is distributive.

It is this fact, more than anything else, which makes the description of Λ_2 so much easier than the case of $\Lambda_{2'}$ dealt with in [3].

Since F' is of class 2, it is easy to see that for each odd prime power p^k the $\underline{\underline{B}}_{p^k}$-subgroup of any subgroup A of F' is just the set of all p^kth powers of elements of A ; accordingly, we shall denote it by A^{p^k} instead of the more cumbersome $\underline{\underline{B}}_{p^k}(A)$. The situation for F itself is not quite so simple: there we do, emphatically, distinguish between the *set* of p^kth powers denoted by F^{p^k} and the *subgroup* $\underline{\underline{B}}_{p^k}(F)$ they generate. Our first preliminary result shows that even this distinction is irrelevant when the odd prime p is not 3 , and provides a (necessarily) weaker but for our purposes adequate variant when $p = 3$.

3.1 If p is a prime and $p > 3$, then $\underline{\underline{B}}_{p^k}(F) = F^{p^k}$, while $\underline{\underline{B}}_{3^{k+1}}(F) \subseteq F^{3^k}$

Proof. The first statement holds not only for F but for every nilpotent group of class less than p , and is familiar in the context of regular p-groups. We shall only sketch a proof for the less familiar second claim. To this end we temporarily abandon F and work in an infinite rank free group G of $\underline{\underline{N}}_4$, freely generated by $x_1, x_2, \ldots$. For $k \geq 0$, put

$$u_2 = x_1 x_2 [x_1, x_2]^{\frac{1}{2}(3^{k+1}-1)} .$$

The Hall-Petrescu Identities (III.9.4 in Huppert [8]) readily yield that there is an element v_2 in $\underline{\underline{N}}_2(G)$ for which

$$x_1^{3^{k+1}} x_2^{3^{k+1}} = u_2^{3^{k+1}} v_2^{3^k} .$$

Induction on n rapidly establishes the existence of elements u_n in G and v_n in $\underline{\underline{N}}_2(G)$ such that

$$x_1^{3^{k+1}} x_2^{3^{k+1}} \dots x_n^{3^{k+1}} = u_n^{3^{k+1}} v_n^{3^k} .$$

As the subgroup of G generated by u_n^3 and v_n has class at most 2, a straightforward calculation within that subgroup then yields

$$x_1^{3^{k+1}} x_2^{3^{k+1}} \dots x_n^{3^{k+1}} = (u_n^3 v_n [u_n^3, v_n]^{\frac{1}{2}(3^k-1)})^{3^k} ,$$

and this proves our claim.

One more piece of folklore before we can start in earnest: if p is an odd prime then there is no fully invariant subgroup of F strictly between F'' and $(F'')^p$. This is proved for $p = 3$ in the (unpublished part of the) thesis [5] of Harris (pp 73-74) by an argument which works equally well when $p > 3$. For $p > 3$ it can, of course, also be extracted from the classification of varieties of groups of exponent p and class less than p, in which context one relies on the fact that even the automorphism group of F acts irreducibly on $F''/(F'')^p$, as a quotient of $GL(4, p)$.

It follows then that if f is an odd integer and p is a prime divisor of f, there is no fully invariant subgroup of F strictly between $(F'')^{f/p}$ and $(F'')^f$. We take this one step further.

3.2 If $V \in \Lambda_2$ and $1 < V \leq F''$ then $V = (F'')^f$ for some

odd positive integer f .

Proof. Since $1 < V \leq F''$, also $1 < V_0 \leq F''$; as F'' is minimal in Λ_0 , we have $V_0 = F''$. By 2.2, the assumption $V \in \Lambda_2$ gives $V_0 = (V_2)_{2'} = V_{2'}$, so V has odd index in F'' . Let f denote the (exact) exponent of F''/V . If $V/(F'')^f$ is nontrivial, it has an element of some odd prime order p . As F'' is free abelian, all elements of order p in $F''/(F'')^f$ lie in $(F'')^{f/p}/(F'')^f$, so $(F'')^f < V \cap (F'')^{f/p} \leq (F'')^{f/p}$. By the preceding discussion this implies that $V \cap (F'')^{f/p} = (F'')^{f/p}$, so $V \geq (F'')^{f/p}$: contrary to the choice of f as the exact exponent of F''/V . Therefore $V/(F'')^f$ must be trivial.

A similar argument will give us the following.

3.3 If $V \in \Lambda_2$ and $F'' < V \leq N$ then $V = N^e F''$ for some odd positive integer e .

Proof. All we need to establish is that if p is an odd prime then there is no fully invariant subgroup of F strictly between $N^p F''$ and N . As F/N is torsionfree, 3.1 ensures that $\underline{\underline{B}}_p{}_2(F) \cap N \leq N^p$, so by the modular law $\underline{\underline{B}}_p{}_2(F)N^pF'' \cap N = N^pF''$. Put $H = F/\underline{\underline{B}}_p{}_2(F)N^pF''$. The natural homomorphism of F onto H would map a fully invariant subgroup of V strictly between N^pF'' and N to a fully invariant subgroup of H strictly between 1 and $\underline{\underline{N}}_3(H)$. However, H is a free group of a variety of metabelian p-groups of class at most 4, with $\underline{\underline{N}}_3(H)$ of exponent p , so one can read off Brisley's classification of such varieties (from [1] if $p > 3$, from [2] if $p = 3$) that no fully invariant

subgroup of H can lie strictly between 1 and $\underline{\underline{N}}_3(H)$. This completes the proof.

We shall need much more detail from Brisley in the end, but this much will suffice in this section. Before we start on the proof of the distributivity of Λ_2, we must recall a little more of the structure of N. Of course, N is free abelian on the basis consisting of the basic commutators of weight 4 (formed with respect to the ordered free generating set $\{x, y, z, t\}$ of F, say); by Witt's Formula, there are 60 of these. Direct inspection shows that precisely 15 of them are not left-normed: those lie in F''. In fact they (freely) generate F'' : for, by a theorem of Magnus (36.32 in Neumann's [13]), the cosets of the other 45 form a free abelian basis of N/F''.

We are now ready to prove the distributivity of Λ_2, along the lines of Section 2 of [11]. The reader is invited to check that the arguments described there can be adapted to prove that if $U, V \in \Lambda_2$ then the sublattice of Λ_2 generated by U, V, and N, is distributive: so Λ_2 is a subdirect product of its sublattices

$$\{W \in \Lambda_2 \mid W \geq N\} \text{ and } \{W \in \Lambda_2 \mid W \leq N\}.$$

The first of these is also a sublattice of Λ (on account of 2.6), and so dual to a sublattice of the lattice of all varieties of nilpotent groups of class at most 3 : hence it is distributive. It remains to prove the distributivity of the second lattice. To this end, it is sufficient to show that if $U, V \in \Lambda_2$ and $U, V \leq N$ then the sublattice of Λ_2 generated by U, V, and F'',

is distributive. Indeed, once this is established we can argue that $\{W \in \Lambda_2 \mid W \leq N\}$ is a subdirect product of $\{W \in \Lambda_2 \mid W \leq F''\}$ and $\{W \in \Lambda_2 \mid F'' \leq W \leq N\}$, and 3.2, 3.3 show that each of these is dual to the distributive lattice Ω described in the introduction. Imitate Section 2 of [10] once more: if the sublattice generated by U, V, F'' in $\{W \in \Lambda_2 \mid W \leq N\}$ were not distributive, one could deduce that F'' and N/F'' had (End F)-admissible, nontrivial, 2-torsionfree sections which were (End F)-isomorphic. This is impossible: for, by 3.2 each nontrivial, (End F)-admissible section of F'' is the direct product of 15 pairwise isomorphic cyclic groups, while by 3.3 the same holds for N/F'' with 45 in place of 15. This completes the proof of the distributivity of Λ_2.

4. Meetirreducibles

Since F is a finitely generated nilpotent group, it has no infinite properly ascending chains of subgroups. As in any distributive lattice with such a chain condition, each element of Λ_2 has a unique expression as an irredundant meet of meetirreducible elements; and, indeed, the lattice can be reconstructed from the poset of its meetirreducible elements. The aim of this section is to determine that poset for Λ_2.

If $V \in \Lambda_2$ and V_0/V is not a p-group for any prime p, then V has a proper meet decomposition $V = \bigcap_p V_p$ with V_p/V the nontrivial Sylow p-subgroups of V_0/V. If V_0/V has exponent p^k (> 1) for some (odd) prime p then one sees from

3.1 that $\underset{=}{B}_{p^{k+1}}(F) \cap V_0 \leq \underset{=}{B}_{p^k}(V_0) \leq V$ and so the modular law gives a meet decomposition $V = V_0 \cap \underset{=}{B}_{p^{k+1}}(F)V$ which is proper unless $\underset{=}{B}_{p^{k+1}}(F)V = V$ or, equivalently, $V_0 = F$. Thus the meetirreducibles of Λ_2 outside Λ_0 all have prime-power index in F. Those which contain F'' correspond to joinirreducible varieties of metabelian p-groups of class at most 4, and hence are known from Brisley's work (see especially the summing up in the first paragraph of page 61 of [2], from which it is an elementary exercise to identify them).

Thus we have narrowed down the real task of this section to the consideration of meetirreducibles V of prime-power index in F, with $V \not\geq F''$. For each odd prime power p^k ($\neq 1$), put

$$B(p^k) = \begin{cases} (F')^{3^k} \underset{=}{B}_{3^{k+1}}(F) & \text{if } p = 3, \\ \underset{=}{B}_{p^k}(F) & \text{if } p > 3. \end{cases}$$

We shall prove that

4.1 each $B(p^k)M$ is meetirreducible, with

4.2 $B(p^k)M \cap F'' = (F')^{p^k}$,

and conversely: if V is a meetirreducible with prime-power index in F and $V \not\geq F''$, by 3.2 we have $V \cap F'' = (F'')^{p^k}$ for some odd prime power p^k, and then

4.3 $V = B(p^k)M$.

We shall use modularity (Dedekind's Law) so frequently that we must do so without reference. Occasionally we appeal to the

distributivity of Λ_2, without formally writing joins in Λ_2 : in those cases the relevant joins are simply products, because 2.6 applies favourably.

Let us start with the proof of 4.2. As F/F' is torsionfree, 3.1 yields that $B(p^k)M \cap F' = (F')^{p^k} M$ (regardless of whether $p = 3$ or $p > 3$). Since F'/F'' is torsionfree, $(F')^{p^k} \cap F'' = (F'')^{p^k}$. Using also the distributivity of Λ_2, we can then argue that

$$B(p^k)M \cap F'' = B(p^k)M \cap F' \cap F'' = (F')^{p^k} M \cap F'' =$$
$$= [(F')^{p^k} \cap F''][M \cap F''] = (F'')^{p^k} .$$

Next we prove 4.3, but this takes much longer; for the duration of this proof, write simply B for $B(p^k)$ where p^k is defined by $V \cap F'' = (F'')^{p^k}$. The distributivity of Λ_2, together with 4.2, gives that

$$VBM \cap VF'' = V(BM \cap F'') = V(F'')^{p^k} = V .$$

As $VF'' > V$ and V is meetirreducible, we must have $VBM = V$: that is,

4.4 $\quad V \geq BM$.

Assume for the moment that

4.5 $\quad V \leq BN$.

We have seen that N/MF'' is a 2-group, while (by the definition of B) F/BMF'' is of odd order, so we must have $N \leq BMF''$ and hence $N = (B \cap N)MF''$. Therefore, by 4.4,

$$V \cap N = V \cap (B \cap N)MF'' = (B \cap N)M(V \cap F'') = (B \cap N)M(F'')^{p^k} ,$$

so 4.2 gives that $V \cap N = (B \cap N)M$. Thus if 4.5 is true then, using 4.4 again, we get

$$V = V \cap BN = B(V \cap N) = B(B \cap N)M = BM ,$$

and this is what we are trying to establish.

The proof of 4.5 proceeds by contradiction. Suppose it is false; then, by 4.4, we have $VN > BN$. Now, VN and BN are verbal subgroups of F corresponding to varieties of nilpotent groups of class at most 3, and all such varieties are well known. In particular, the variety corresponding to BN is joinirreducible, and its unique maximal subvariety is defined by the extra law $[x_2, x_1, x_1]^{p^{k-1}} = 1$. It follows that $[y, x, x]^{p^{k-1}} = vw$ for some v in V and w in N. Consider the endomorphisms α and δ of F which leave x, z, and t unchanged while $y\alpha = [z, y]$ and $y\delta = 1$. Note that α and δ agree on N: for a basic commutator of weight four is mapped to 1 or left fixed by α depending only on whether y does or does not occur among its entries, and the same is true for δ. We have that $(v\delta)(w\delta) = 1$, for $[y, x, x]\delta = 1$; hence

$$[z, y, x, x]^{p^{k-1}} = (vw)\alpha = (v\alpha)(w\alpha) = (v\alpha)(w\delta) = (v\alpha)(v\delta)^{-1} \in V .$$

On the other hand,

$$[y, x, x, z]^{p^{k-1}} = [vw, z] = [v, z] \in V .$$

Since the fully invariant subgroup closure of $[z, y, x, x]$ and $[y, x, x, z]$ in F is N (Heineken [6]; III.6.9 in Huppert [8]), it follows that $N^{p^{k-1}} \leq V$. This contradicts $V \cap F'' = (F'')^{p^k}$, and thereby completes the proofs of 4.5 and 4.3.

We have left the proof of 4.1 to the last. Consider the expression of $B(p^k)M$ as a meet of meetirreducibles $V(1), \ldots, V(n)$. Then $(F'')^{p^k} = B(p^k)M \cap F'' = \bigcap_i (V(i) \cap F'')$. By 3.2, the fully

invariant subgroup of F between $(F'')^{p^k}$ and F form a chain, so we must be able to choose j so that $V(j) \cap F'' = (F'')^{p^k}$. Then $V(j)$ is a meetirreducible which is not isolated, hence by the introductory discussion of this section it must have prime-power index in F; as it does not contain F'', 4.3 applies to it: hence $V(j) = B(p^k)M$. This completes the proof of 4.1.

All that remains is to add in the meetirreducibles from Λ_0 and the meetirreducibles one obtains from Brisley (loc. cit). The result is that Λ_2 has precisely the following meetirreducible elements:

F, F', $\underline{\underline{N}}_2(F)$, N, F'', M,

$\underline{\underline{B}}_{p^k}(F)F'$, $\underline{\underline{B}}_{p^k}(F)\underline{\underline{N}}_2(F)$, $\underline{\underline{B}}_{p^k}(F)N$ with $p \geq 3$, $k \geq 1$,

$\underline{\underline{B}}_{p^k}(F)F''$, $\underline{\underline{B}}_{p^k}(F)M$ with $p > 3$, $k \geq 1$, and

$\underline{\underline{B}}_{3^{k+1}}(F)\underline{\underline{B}}_{3^k}(F')N$, $\underline{\underline{B}}_{3^{k+1}}(F)\underline{\underline{B}}_{3^k}(F')F''$, $\underline{\underline{B}}_{3^{k+1}}(F)\underline{\underline{B}}_{3^k}(F')M$ with $k \geq 1$.

Obviously, two of these subgroups are comparable if and only if that is directly visible from the way we have written them.

5. Conclusion

Our final task is to prove the main result stated in the introduction. Note that this result will achieve the aims we set in Section 2. For, if $V \in \Lambda_2$ and we change to 1 each nonzero entry of the corresponding (a, b, c, d, e, f), we get another admissible set of parameters; the subgroup U corresponding to this lies in Λ_0, and the exponent of U/V divides the product of the original nonzero parameters: so V_0 is this U, and

we do have an estimate on the exponent of V_0/V .

We shall make use of a simple fact from lattice theory (see, for instance, §21 of Hermes [7]): in a distributive lattice which satisfies the ascending chain condition, each element can be written in one and only one way as the meet of pairwise incomparable meetirreducibles.

To fit our context, let $\mho$ denote the dual of Ω , and Δ the dual of the sublattice of Ω^6 described in the introduction: thus Δ is a sublattice of $\mho^6$, and we shall never refer to Ω or Ω^6 again. Define $\varphi : \mho^6 \to \Lambda$ by $(a, b, c, d, e, f)\varphi = U$ where U is the fully invariant subgroup of F generated as such by x^a, $[y, x]^b$, $[y, x, z]^c$, $[y, x, x]^d$, $[y, x, x, y]^e$, $[[t, z], [y, x]]^f$, and $[t, x, y, z]^{ef}$. What we have to prove amounts to the claim that restriction of φ yields a lattice-isomorphism $\Delta \to \Lambda_2$. In fact, we shall also obtain the inverse of this lattice-isomorphism. Define $\psi : \Lambda_2 \to \mho^6$, $U \mapsto U\psi = (a, b, c, d, e, f)$ by choosing a as the order of xU in F/U (or as 0 if that order is infinite), b as the order of $[y, x]U$ in F/U , and so on. Our full claim is that ψ maps Λ_2 (lattice) isomorphically onto Δ , and $\psi\varphi$ is the identity map on Λ_2 .

The first step of the proof is to note that by its definition φ is a poset-homomorphism, and that ψ is even a meet-homomorphism (as the order of an element of F modulo $U \cap V$ is the least commom multiple of its orders modulo U and V) .

The second step is to check that $\mho^6\varphi \subseteq \Lambda_2$; that is, that if

$(a, b, c, d, e, f)\varphi = U$ then $U_2 = U$. This is done case by case, according to which is the first (if any) nonzero entry in (a, b, c, d, e, f) . Take, for instance, the case $a = b = c = 0 \neq d$, when $[y, x, x]^d \in U \leq \underline{\underline{N}}_2(F)$. Let A/U be the fully invariant subgroup of F/U defined by $[y, x, x]U$: since this element has odd order (dividing d), $|A/U|$ is odd. On the other hand, $\underline{\underline{N}}_2(F)/A$ has exponent dividing 3, so $|\underline{\underline{N}}_2(F)/U|$ is odd, and hence $U \in \Lambda_2$. The other cases are very much easier; we leave them to the reader.

Henceforth we may, and shall, regard φ as a map from $\mathfrak{V}^6$ to Λ_2 .

For the third step, note that $g\varphi\psi \geq g$ for all g in $\mathfrak{V}^6$, simply by the definitions of φ and ψ , and that $U\psi\varphi \leq U$ for all U in Λ_2 . The second claim needs only that $M^e(F'')^f \leq U$ implies $N^{ef} \leq U$: this holds because $(MF'')^{ef} \leq M^e(F'')^f$ so $N/M^e(F'')^f$ has exponent dividing $4ef$ (recall $N^4 \leq MF''$) while $N/N \cap U$ has no element of order 2. Thus $(U\psi)\varphi\psi \geq U\psi$ by the first comment, while $(U\psi\varphi)\psi \leq U\psi$ by the second comment and the order-preserving nature of ψ : so we have that

$$\psi\varphi\psi = \psi \ .$$

Let Γ denote the set of the meetirreducible elements of Λ_2 (listed at the end of the previous section). Our fourth step is to prove that $\Gamma\psi \subseteq \Delta$ and $\psi\varphi$ acts identically on Γ . For the V in Γ with F/V of prime-power order and $V \geq F''$, which we took from Brisley's work, this has (at least implicitly) been

done by Brisley. For the V in $\Gamma \cap \Lambda_0$, this is simply a matter of inspection. For the other V in Γ, we know from 4.3 that $V = B(p^k)M$; put $V\psi = (a, b, c, d, e, f)$. Direct from the definitions of $B(p^k)$ and ψ, we see that

$$V\psi \geq \begin{cases} (3^{k+1}, 3^k, 3^k, 3^k, 1, 3^k) & \text{if } p = 3 \\ (p^k, p^k, p^k, p^k, 1, p^k) & \text{if } p > 3 . \end{cases}$$

Thus $e = 1$; from 4.2, we know that $f = p^k$. As to the other parameters, use that ψ respects order, that $B(p^k)N \geq V$, and that $[B(p^k)N]\psi$ is known from Brisley (or indeed from the facts on varieties of nilpotent groups of class at most 3); and conclude that the inequality displayed above is in fact an equality. It is then immediate that $V\psi \in \Delta$ and $V\psi\varphi = V$.

The fifth step is left to the reader: determine all the meetirreducibles in Δ, and verify that the set they form is precisely $\Gamma\psi$.

The proof of the main result can now be completed quickly. Since $\Gamma\psi$ generates Δ as a meet-semilattice and ψ is a meet-homomorphism, $\Lambda_2\psi = \Delta$. Since φ and ψ are poset-homomorphisms and $\psi\varphi$ is the identity map on Γ, their restrictions to $\Gamma\psi$ and Γ are poset-isomorphisms. If we can establish that $\psi\varphi$ is the identity map, the same argument will now give that ψ and the restriction of φ to Δ are poset-isomorphisms, and it is well known that all poset-isomorphisms of lattices are lattice-isomorphisms.

For the final step, suppose that $U\psi\varphi \neq U$ for some U in Λ_2 : all we have to do is to show that this leads to a contradiction. Write $U\psi\varphi = \bigcap_i V(i)$ and $U = \bigcap_j W(j)$ with the $V(i)$ pairwise incomparable elements of Γ, and the $W(j)$ also pairwise incomparable elements of Γ. As $U\psi\varphi \neq U$, the set of the $V(i)$ is not the set of the $W(j)$. Since ψ acts as poset-isomorphism from Γ to the set of meetirreducibles in Δ, the $V(i)\psi$ from a set of pairwise incomparable meetirreducible elements in Δ, and the $W(j)\psi$ form a different set of pairwise incomparable meetirreducible elements. Yet, because ψ is a meet-homomorphism and $\psi\varphi\psi = \psi$,

$$\bigcap_i V(i)\psi = U\psi\varphi\psi = U\psi = \bigcap_j W(j)\psi .$$

This contradicts the uniqueness of expressions as meets of pairwise incomparable meetirreducibles in Δ (which obviously satisfies the ascending chain condition), and so completes the proof.

REFERENCES

[1] Warren Brisley, "On varieties of metabelian p-groups and their laws", *J. Austral. Math. Soc.* 7 (1967), 64-80.

[2] Warren Brisley, "Varieties of metabelian p-groups of class p , p + 1 ", *J. Austral. Math. Soc.* 12 (1971), 53-62.

[3] Patrick Fitzpatrick, "Varieties of nilpotent groups of class at most four" (PhD thesis, Australian National University, Canberra, 1980: submitted).

[4] N.D. Gupta and M.F. Newman, "On metabelian groups", *J. Austral. Math. Soc.* 6 (1966), 362-368.

[5] L.F. Harris, "Varieties and section closed classes of groups", (PhD thesis, Australian National University, Canberra, 1973).

[6] Hermann Heineken, "Über ein Levisches Nilpotenzkriterium", *Arch. Math.* 12 (1961), 176-178.

[7] Hans Hermes, *Einführung in die Verbandstheorie* (Die Grundlehren der mathematischen Wissenschaften, 73. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1955).

[8] B. Huppert, *Endliche Gruppen I* (Die Grundlehren der mathematischen Wissenschaften, 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[9] Bjarni Jonsson, "Varieties of groups of nilpotency three", *Notices Amer. Math. Soc.* 13 (1966), 488.

[10] A.A. Kljačko, "Varieties of p-groups of small class" (Russian), *Ordered Sets and Lattices* No. 1, 31-42 (Izdat. Saratov. Univ., Saratov, 1971).

[11] L.G. Kovács, "Varieties of nilpotent groups of small class", *Topics in algebra* (Proc. 18th SRI [M.F. Newman, Ed.]. Lecture Notes in Mathematics, 697, 205-229. Springer-Verlag, Berlin, Heidelberg, New York, 1978).

[12] L.G. Kovács, "The thirty-nine varieties", *The Math. Scientist* 4 (1979), 113-128.

[13] Hanna Neumann, *Varieties of Groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 37. Springer-Verlag, Berlin, Heidelberg, New York, 1967).

[14] Paul Pentony, "Laws in torsion free nilpotent varieties" (PhD thesis, Australian National University, Canberra, 1970). See also: Abstract, *Bull. Austral. Math. Soc.* 5 (1971), 283-284.

[15] V.N. Remeslennikov, "Two remarks on 3-step nilpotent groups" (Russian), *Algebra i Logika Sem.* 4 (1965), no. 2, 59-65.

[16] Robert M. Thrall, "A note on a theorem by Witt", *Bull. Amer. Math. Soc.* 47 (1941), 303-308.

Department of Mathematics,
Institute of Advanced Studies,
Australian National University,
Canberra, ACT, Australia.

First author's present address:
University College,
Cork,
Eire.